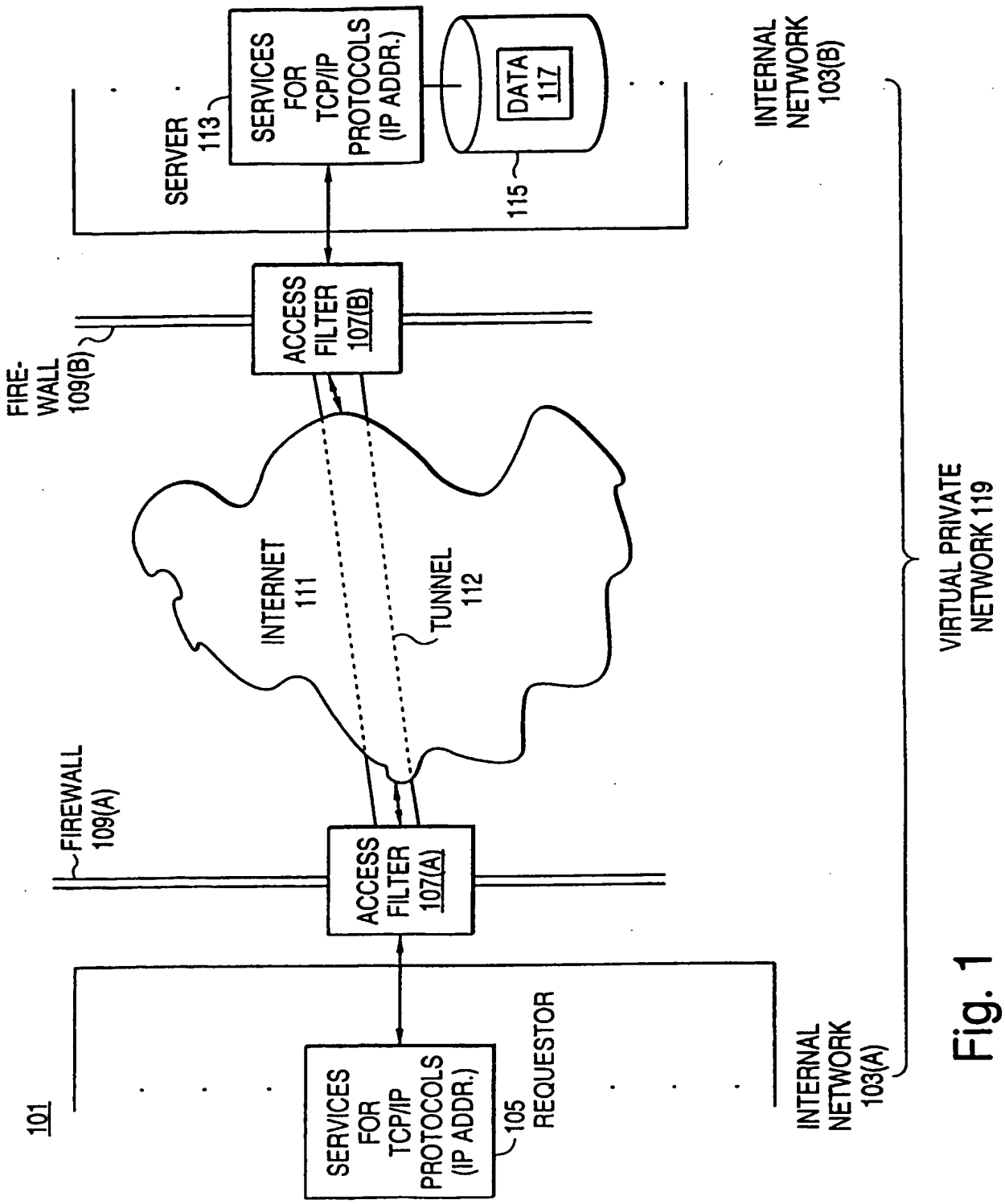

SERVER 113
SERVICES FOR TCP/IP PROTOCOLS (IP ADDR.)
DATA 117
115
INTERNAL NETWORK 103(B)
FIRE-WALL 109(B)
ACCESS FILTER 107(B)
INTERNET 111
TUNNEL 112
FIREWALL 109(A)
ACCESS FILTER 107(A)
VIRTUAL PRIVATE NETWORK 119
101
SERVICES FOR TCP/IP PROTOCOLS (IP ADDR.)
105 REQUESTOR
INTERNAL NETWORK 103(A)

Fig. 1

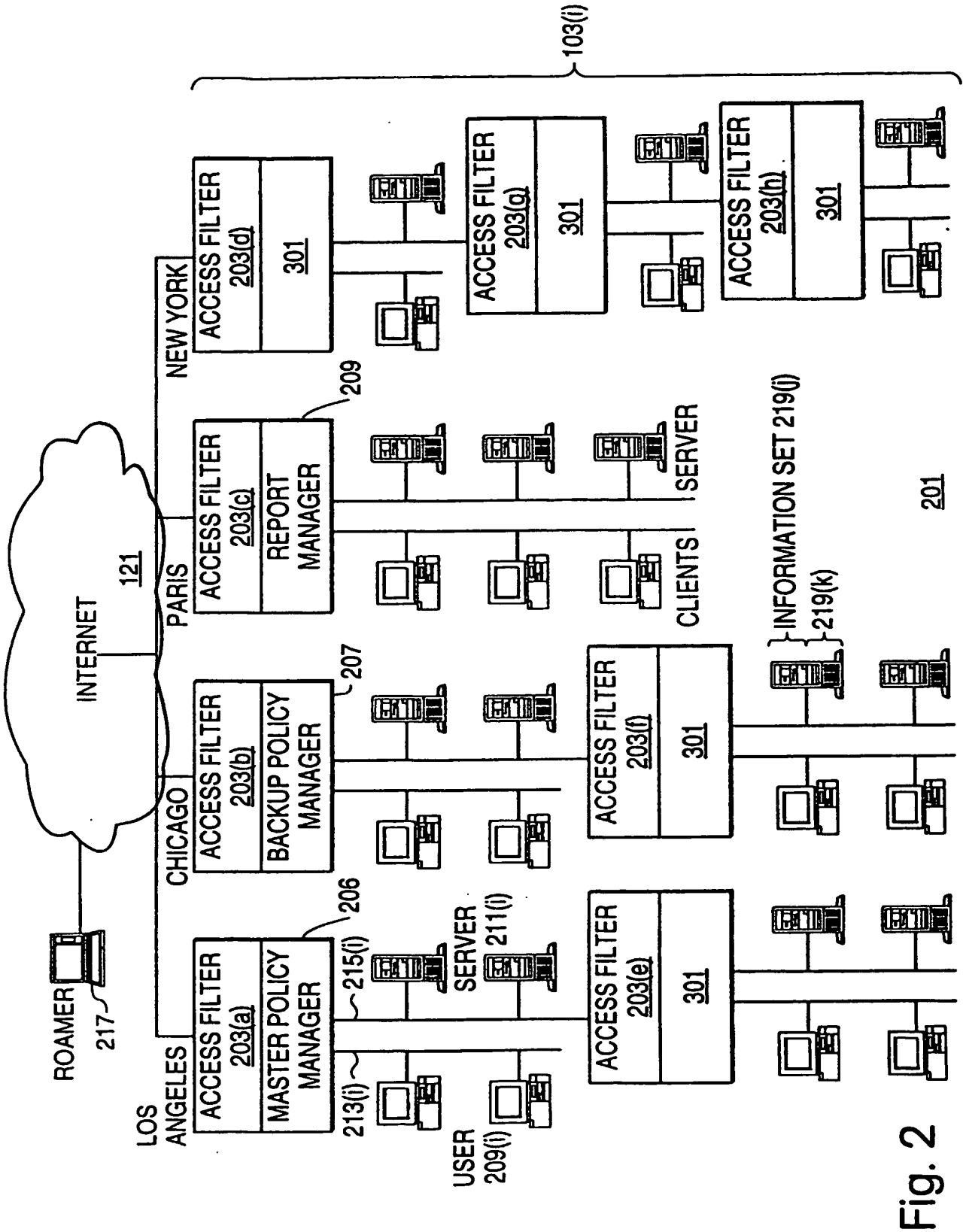

103(i)
ACCESS FILTER 203(d)
301
NEW YORK
ACCESS FILTER 203(g)
301
ACCESS FILTER 203(h)
301
209
ACCESS FILTER 203(c)
REPORT MANAGER
PARIS
SERVER
CLIENTS
INFORMATION SET 219(j)
219(k)
INTERNET
121
201
207
ACCESS FILTER 203(b)
BACKUP POLICY MANAGER
CHICAGO
ACCESS FILTER 203(f)
301
206
ACCESS FILTER 203(a)
MASTER POLICY MANAGER
215(i)
SERVER 211(i)
ACCESS FILTER 203(e)
301
ROAMER
217
LOS ANGELES
213(i)
USER 209(i)

Fig. 2

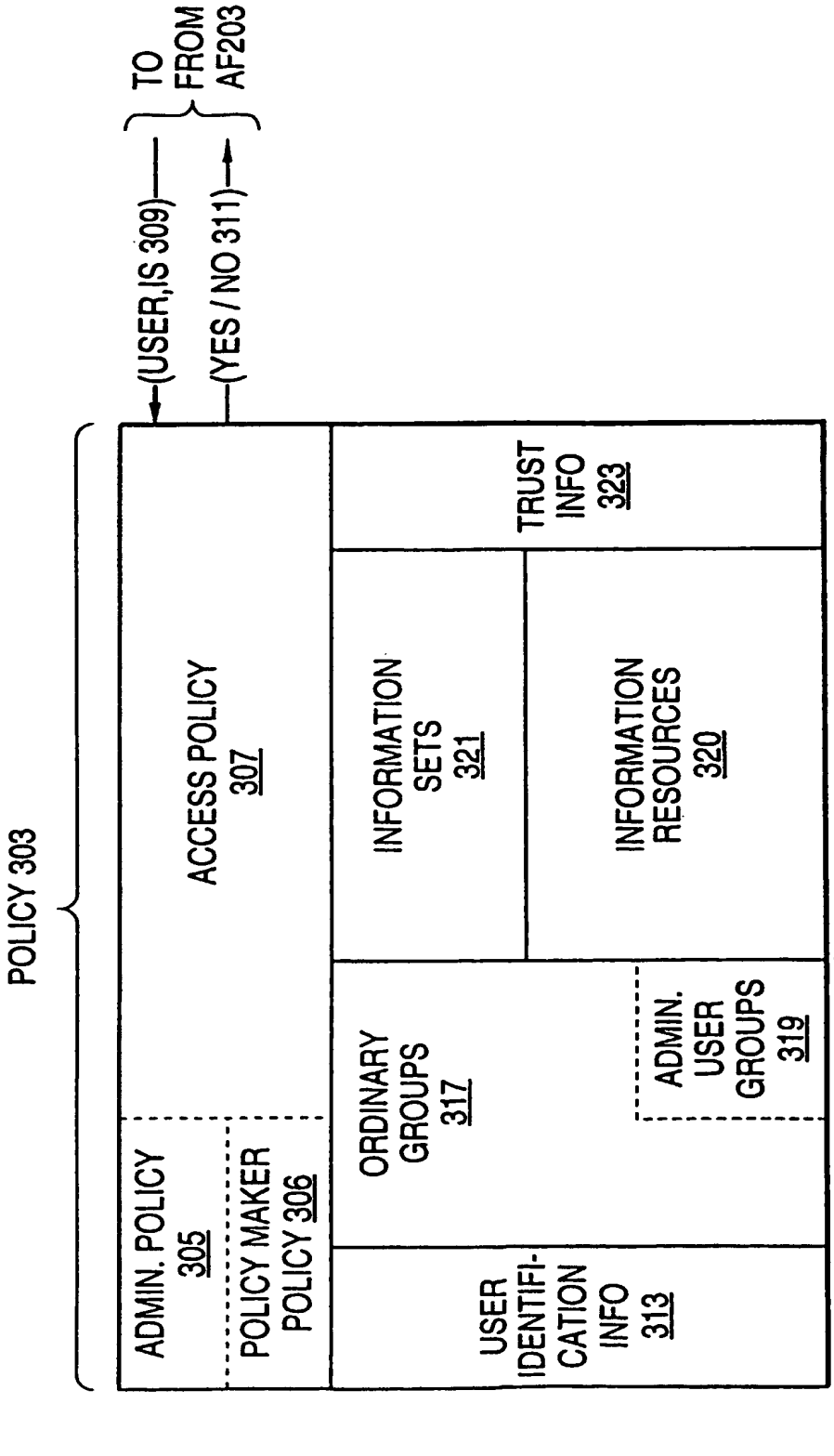

TO AF203
FROM AF203
(USER,IS 309)
(YES / NO 311)
POLICY 303
ADMIN. POLICY 305
POLICY MAKER POLICY 306
ACCESS POLICY 307
USER IDENTIFI-CATION INFO 313
ORDINARY GROUPS 317
ADMIN. USER GROUPS 319
USER GROUPS 315
INFORMATION SETS 321
INFORMATION RESOURCES 320
TRUST INFO 323
301

Fig. 3

10/019101

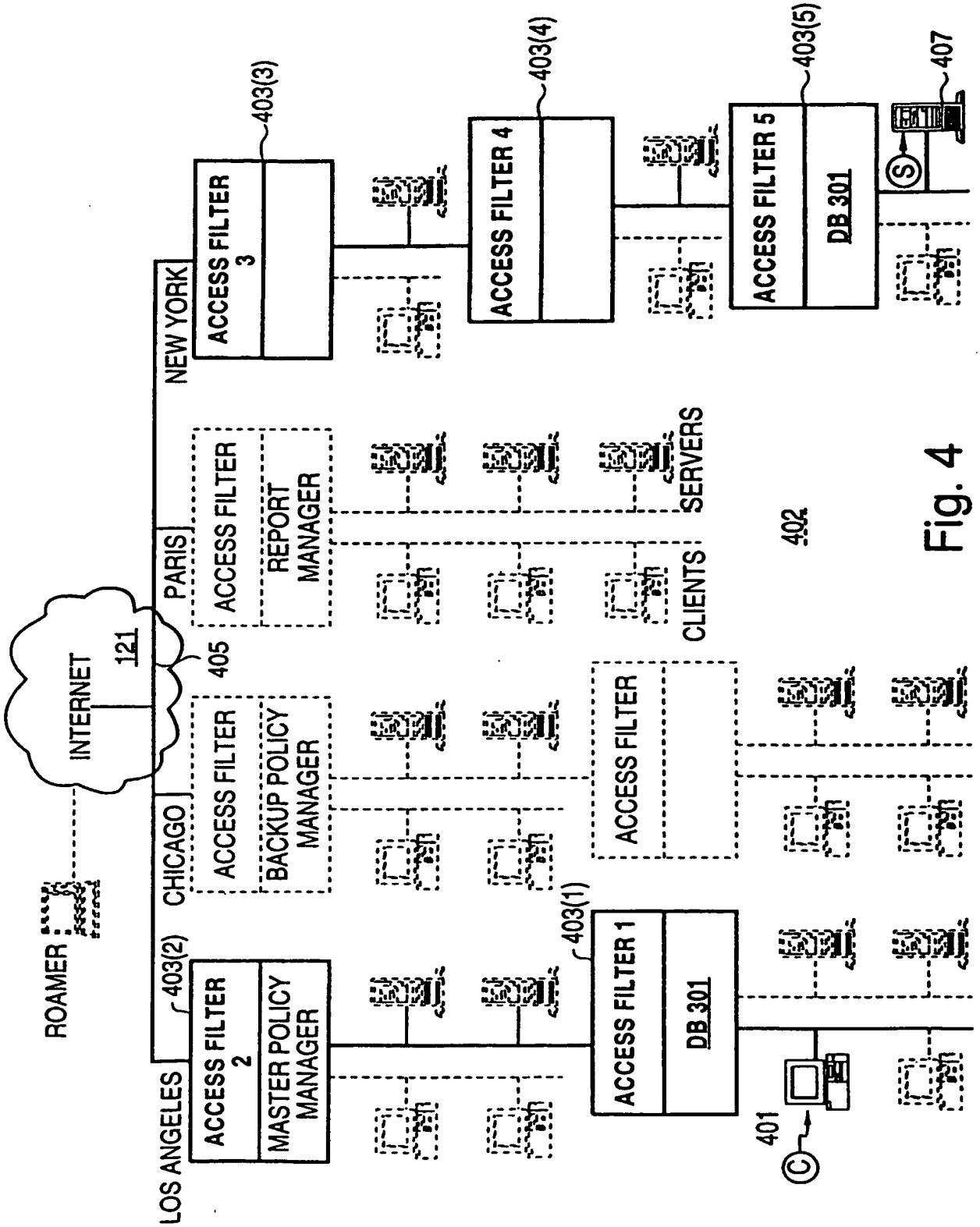


Fig. 4

Docket Retrieval

10/019101

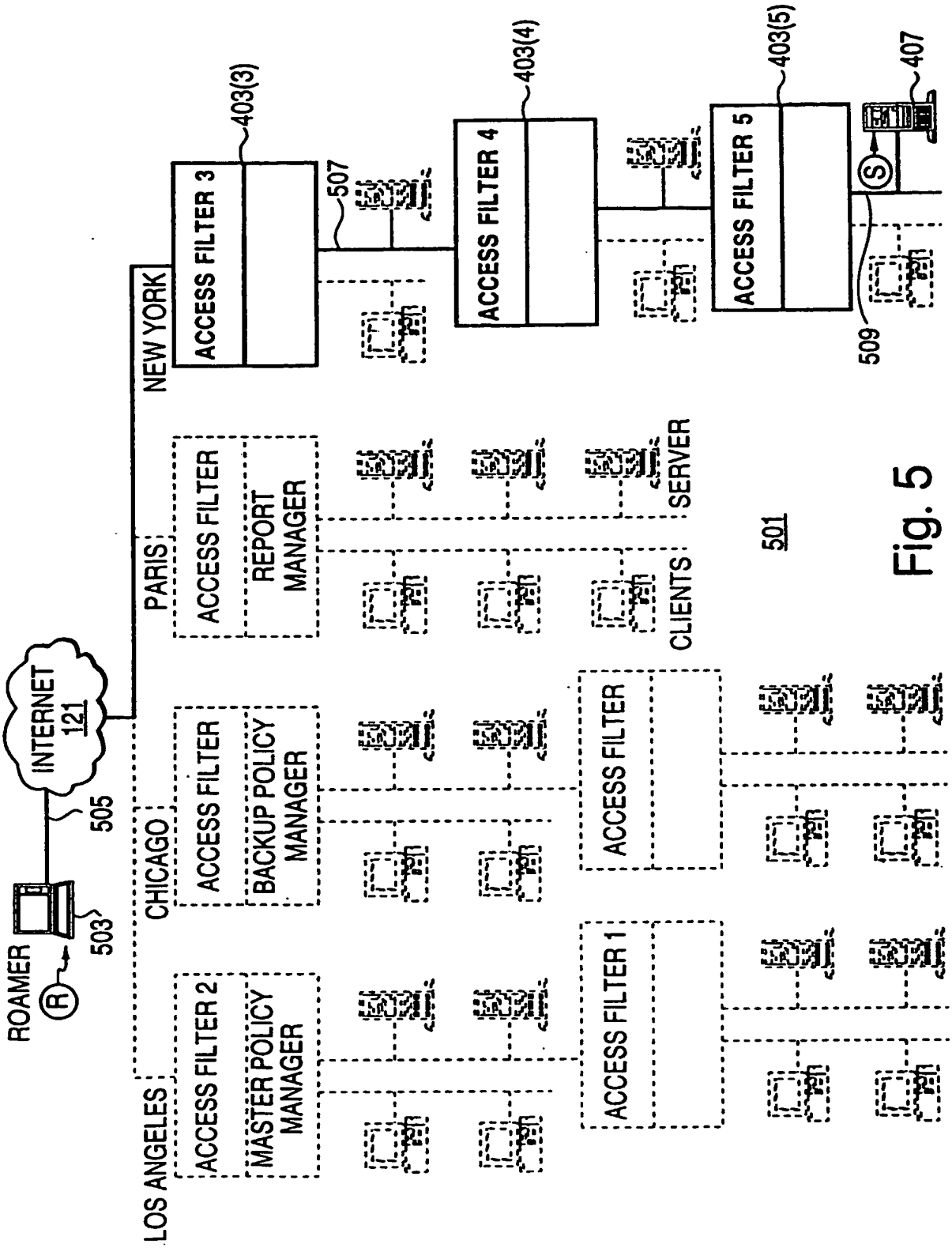


Fig. 5

Trust / Data Sensitivity Level	Minimum Encryption	Minimum Authentication	
Top secret	3DES	Certificate via SKIP	609(1)
Secret	DES	Certificate via SKIP	609(2)
Private	RC4-40	Windows ID	609(3)
Public	None	None	609(4)

601

603 609 607

Fig. 6

10/019101

10/019101

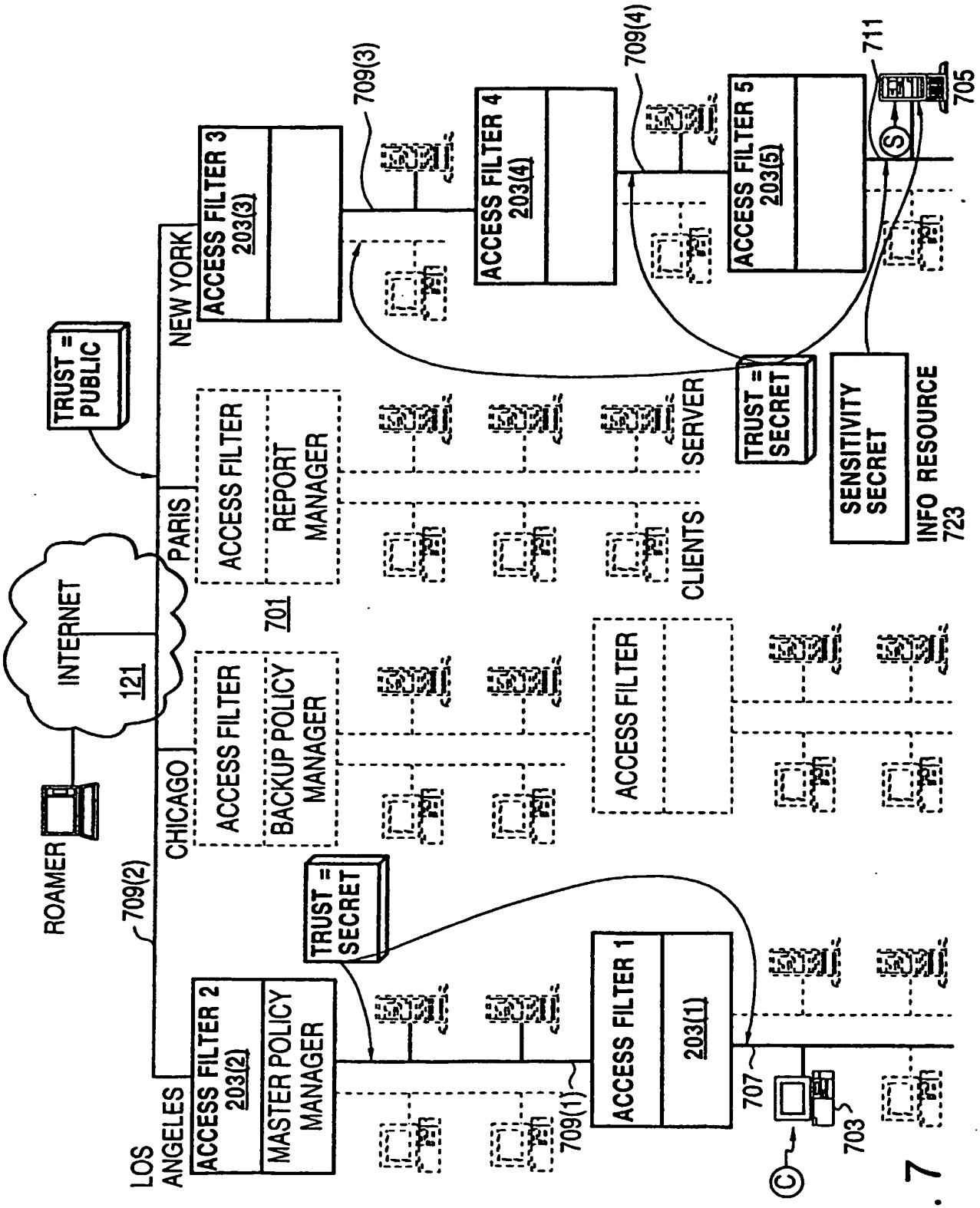


Fig. 7

10/019101

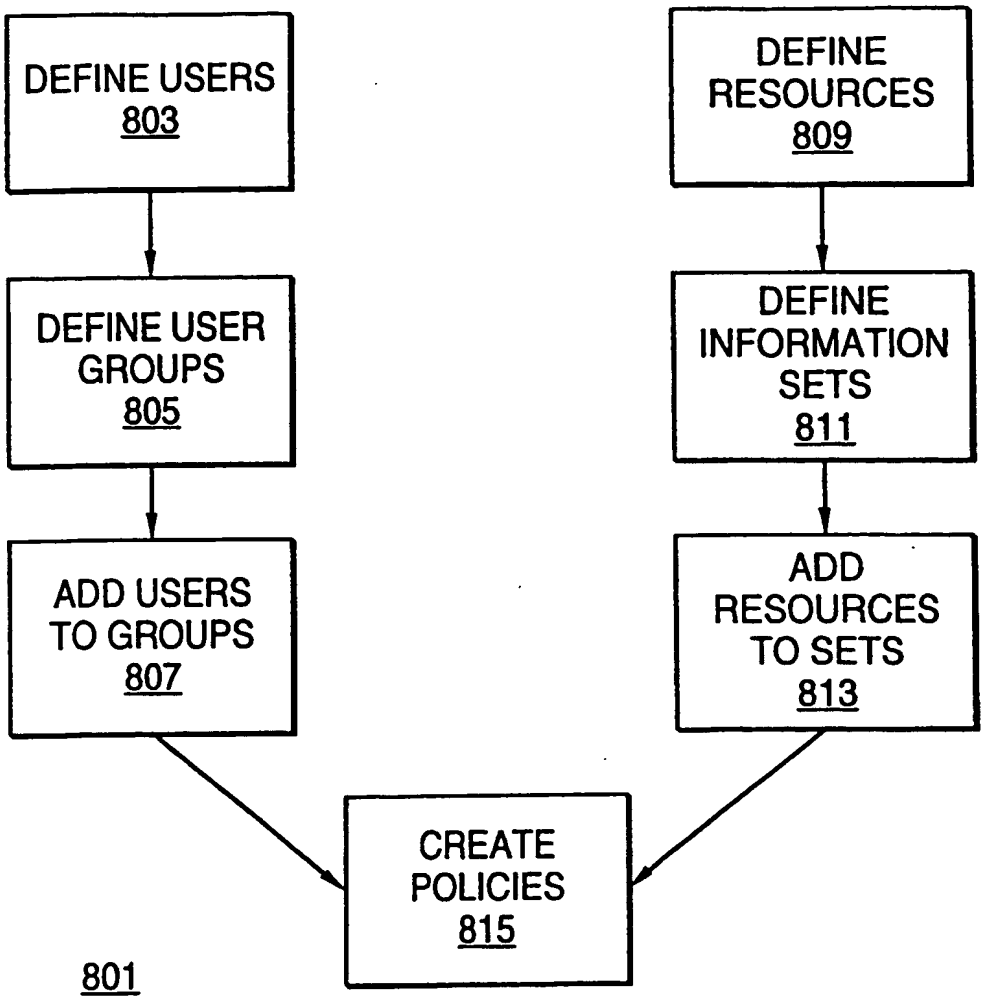


Fig. 8

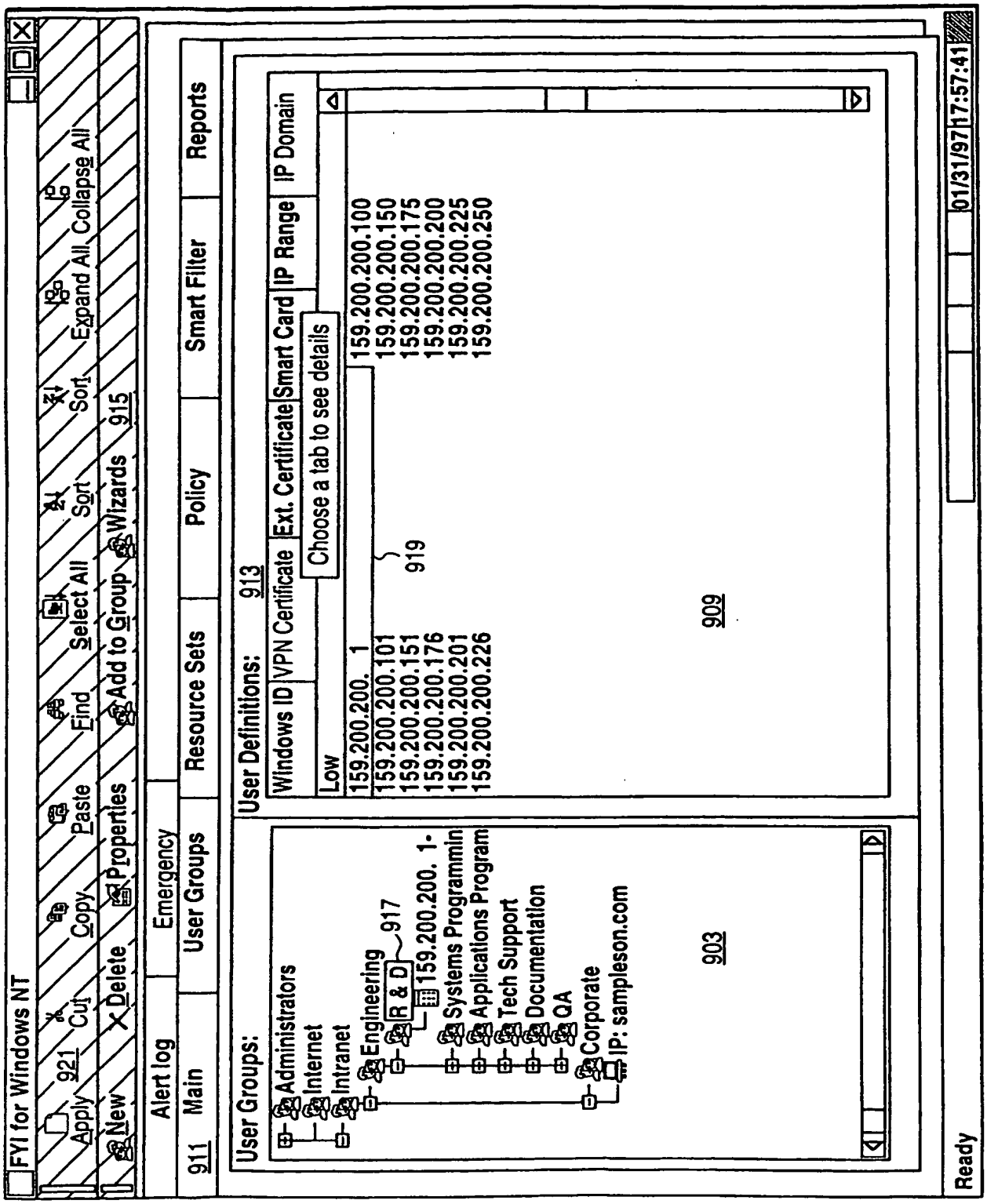

901
FYI for Windows NT
Apply
921
Cut
Copy
Paste
Find
Select All
Sort
Sort
Expand All
Collapse All
New
Delete
Properties
Add to Group
Wizards
915
Alert log
Emergency
911 Main
User Groups
Resource Sets
Policy
Smart Filter
Reports
User Groups:
Administrators
Internet
Intranet
Engineering
R & D
917
159.200.200. 1-
Systems Programmin
Applications Program
Tech Support
Documentation
QA
Corporate
IP: sampleson.com
903
User Definitions:
913
Windows ID
VPN Certificate
Ext. Certificate
Choose a lab to see details
Smart Card
IP Range
IP Domain
Low
159.200.200. 1
159.200.200.101
159.200.200.151
159.200.200.176
159.200.200.201
159.200.200.226
919
159.200.200.100
159.200.200.150
159.200.200.175
159.200.200.200
159.200.200.225
159.200.200.250
909
Ready
01/31/97
17:57:41

Fig. 9

1U/019101

Docket - Undefined

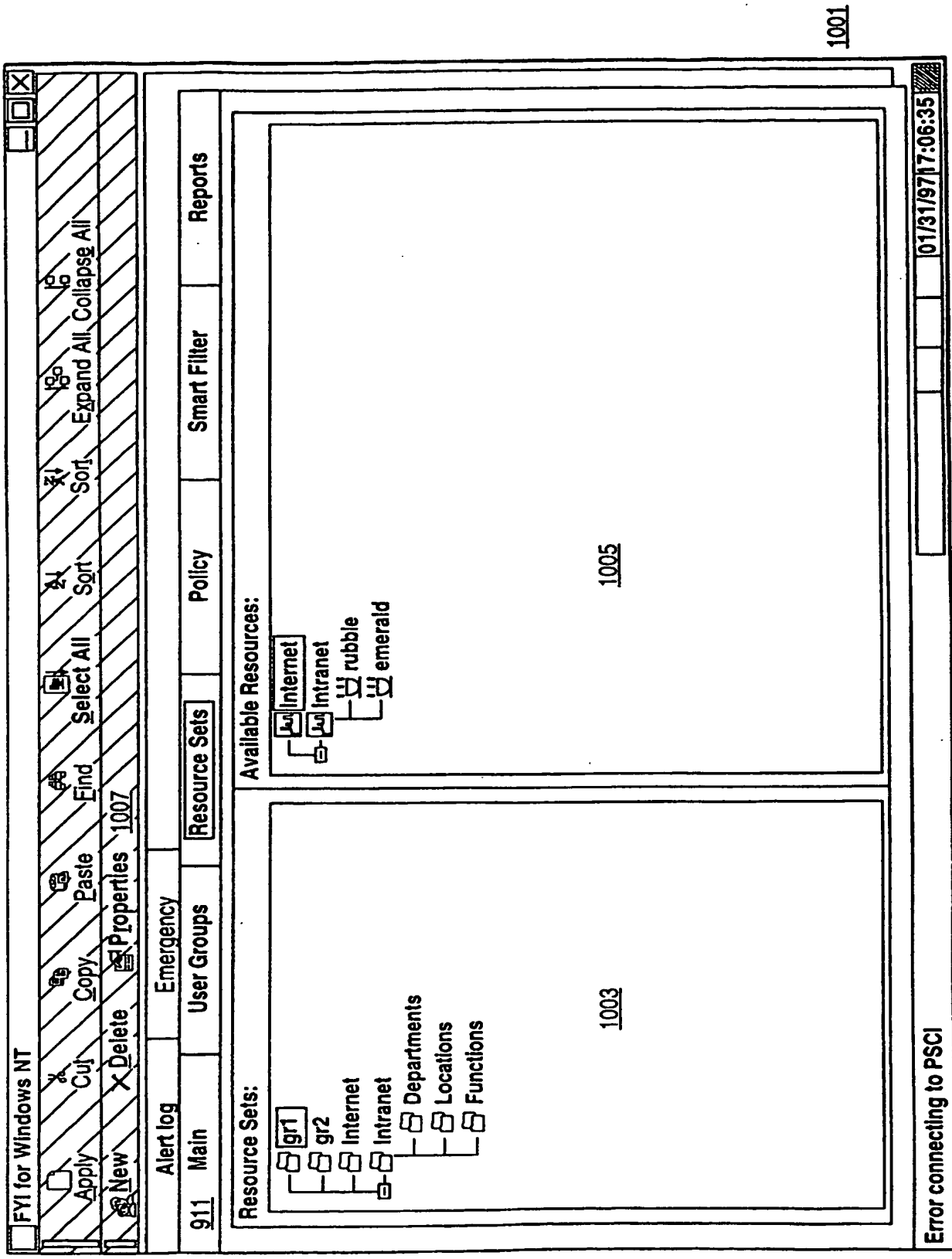


Fig. 10

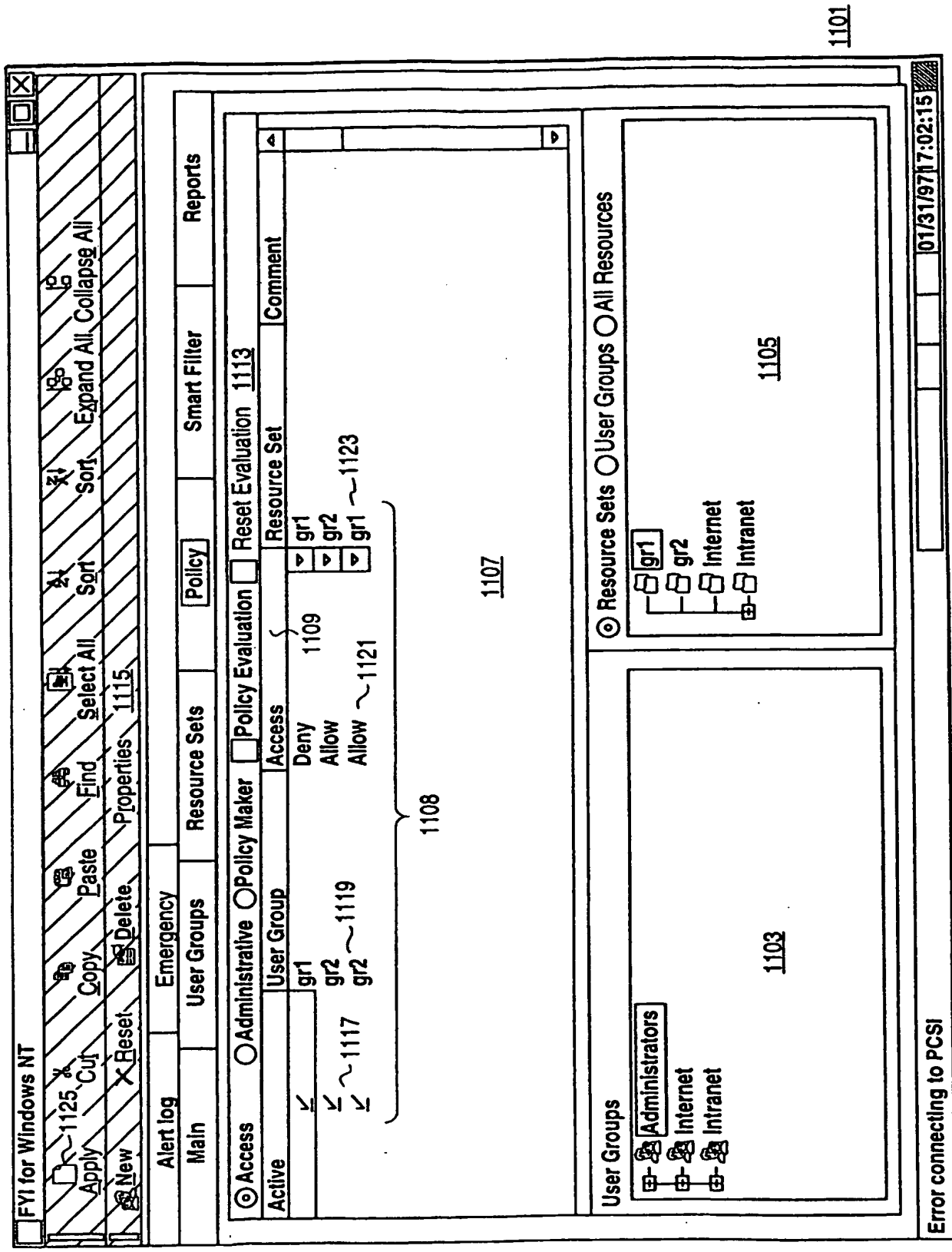

1101
FYI for Windows NT
Cut
Copy
Paste
Find
Select All
Sort
Expand All
Collapse All
Apply
New
Reset
Delete
Properties
1115
Alert log
Emergency
Main
User Groups
Resource Sets
Policy
Smart Filter
Reports
Access
Administrative
Policy Maker
Policy Evaluation
Reset Evaluation
1113
Active
User Group
Access
Resource Set
Comment
gr1
gr2
Deny
Allow
Allow
gr1
gr2
gr2
gr1
1117
1119
1121
1123
1109
1108
1107
Resource Sets
User Groups
All Resources
gr1
gr2
Internet
Intranet
1105
User Groups
Administrators
Internet
Intranet
1103
Error connecting to PCSI
01/31/97 17:02:15

Fig. 11

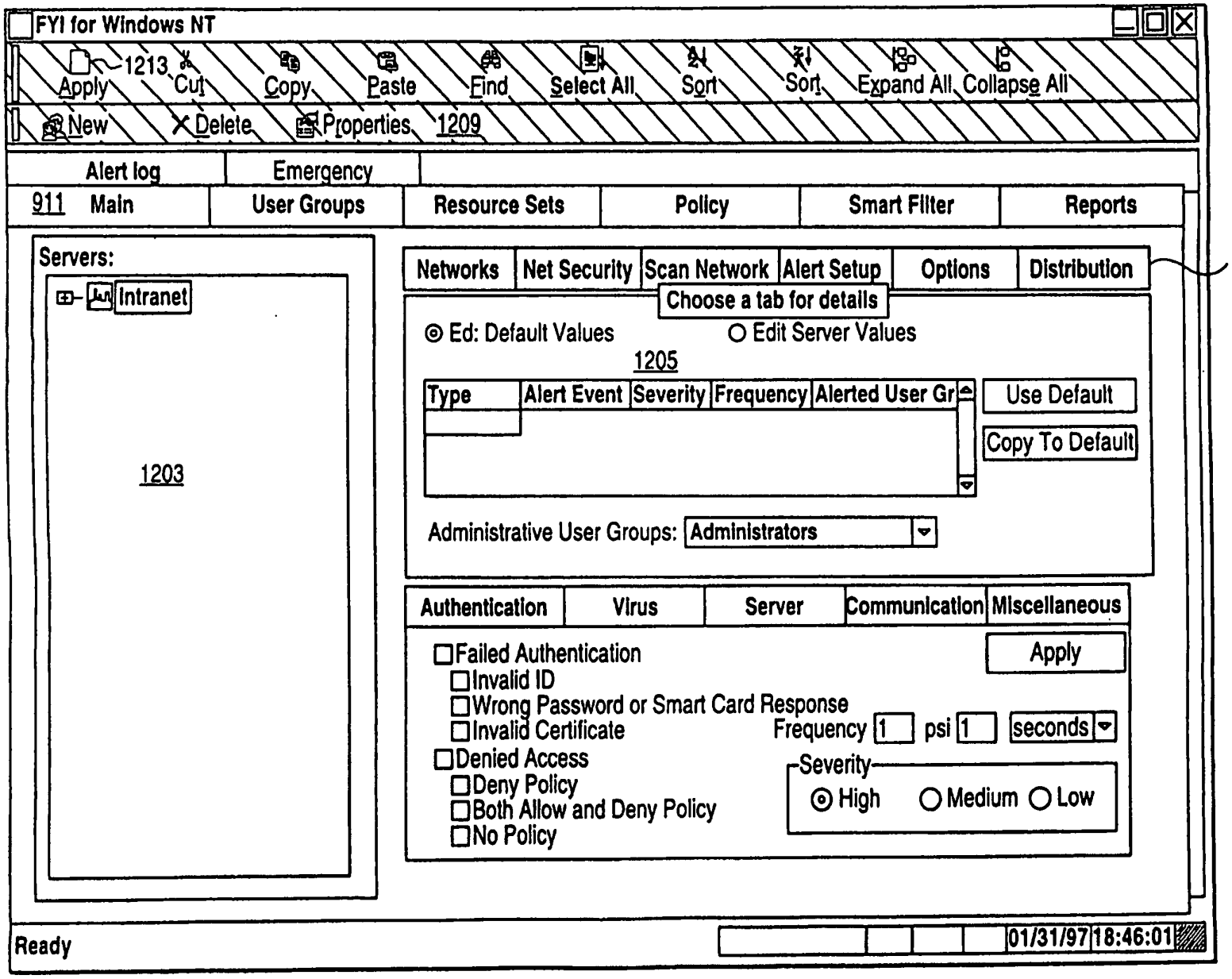


Fig. 12

10/019101

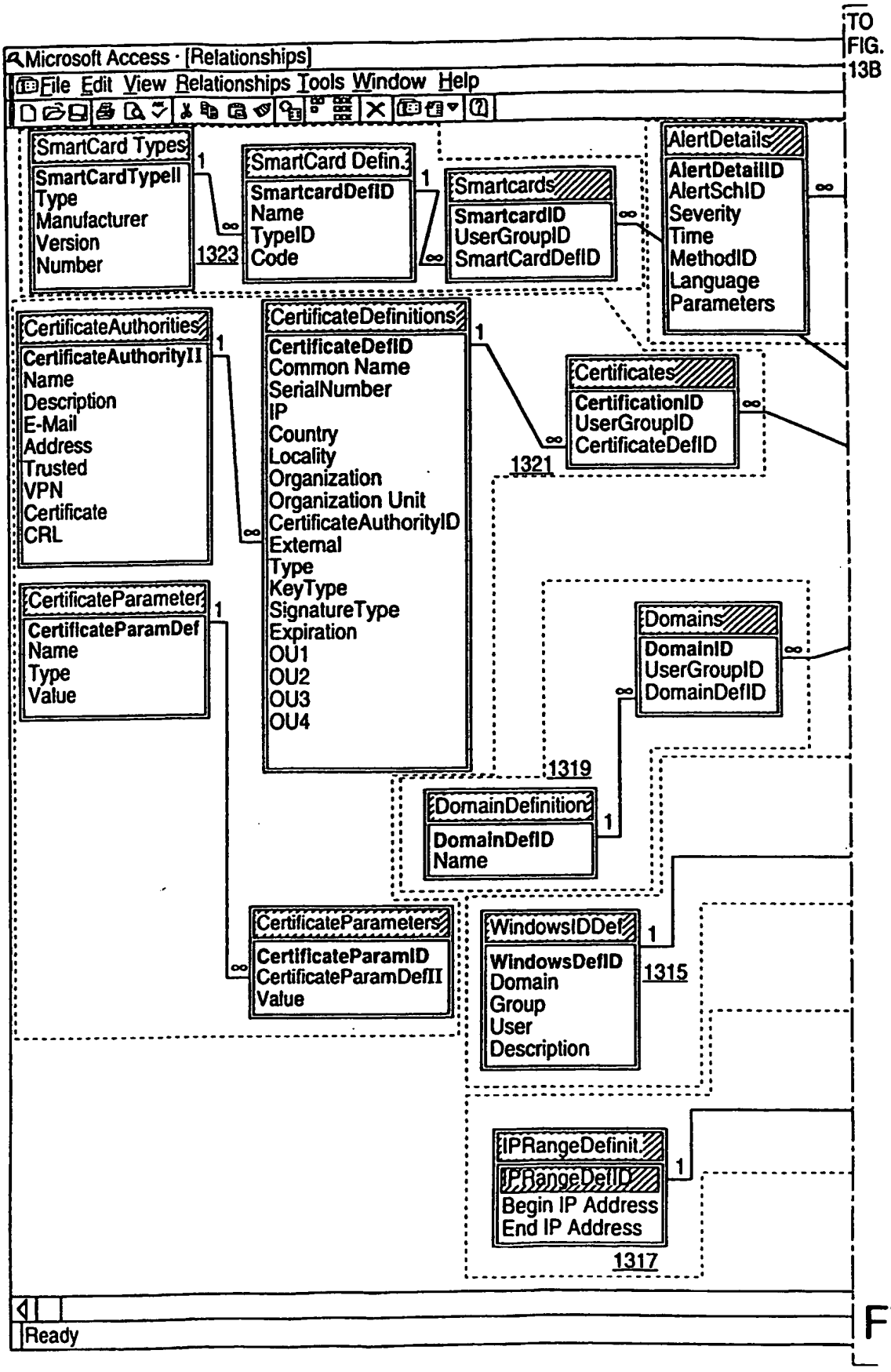

TO FIG. 13B
Microsoft Access - [Relationships]
File Edit View Relationships Tools Window Help
SmartCard Types
SmartCardTypeII
Type
Manufacturer
Version
Number
SmartCard Defin...
SmartcardDefID
Name
TypeID
Code
Smartcards
SmartcardID
UserGroupID
SmartCardDefID
AlertDetails
AlertDetailID
AlertSchID
Severity
Time
MethodID
Language
Parameters
CertificateAuthorities
CertificateAuthorityII
Name
Description
E-Mail
Address
Trusted
VPN
Certificate
CRL
CertificateDefinitions
CertificateDefID
Common Name
SerialNumber
IP
Country
Locality
Organization
Organization Unit
CertificateAuthorityID
External
Type
KeyType
SignatureType
Expiration
OU1
OU2
OU3
OU4
Certificates
CertificationID
UserGroupID
CertificateDefID
1321
CertificateParameter
CertificateParamDef
Name
Type
Value
Domains
DomainID
UserGroupID
DomainDefID
1319
DomainDefinition
DomainDefID
Name
CertificateParameters
CertificateParamID
CertificateParamDefII
Value
WindowsIDDef
WindowsDefID
Domain
Group
User
Description
1315
IPRangeDefinit...
IPRangeDefID
Begin IP Address
End IP Address
1317
Ready

Fig. 13A

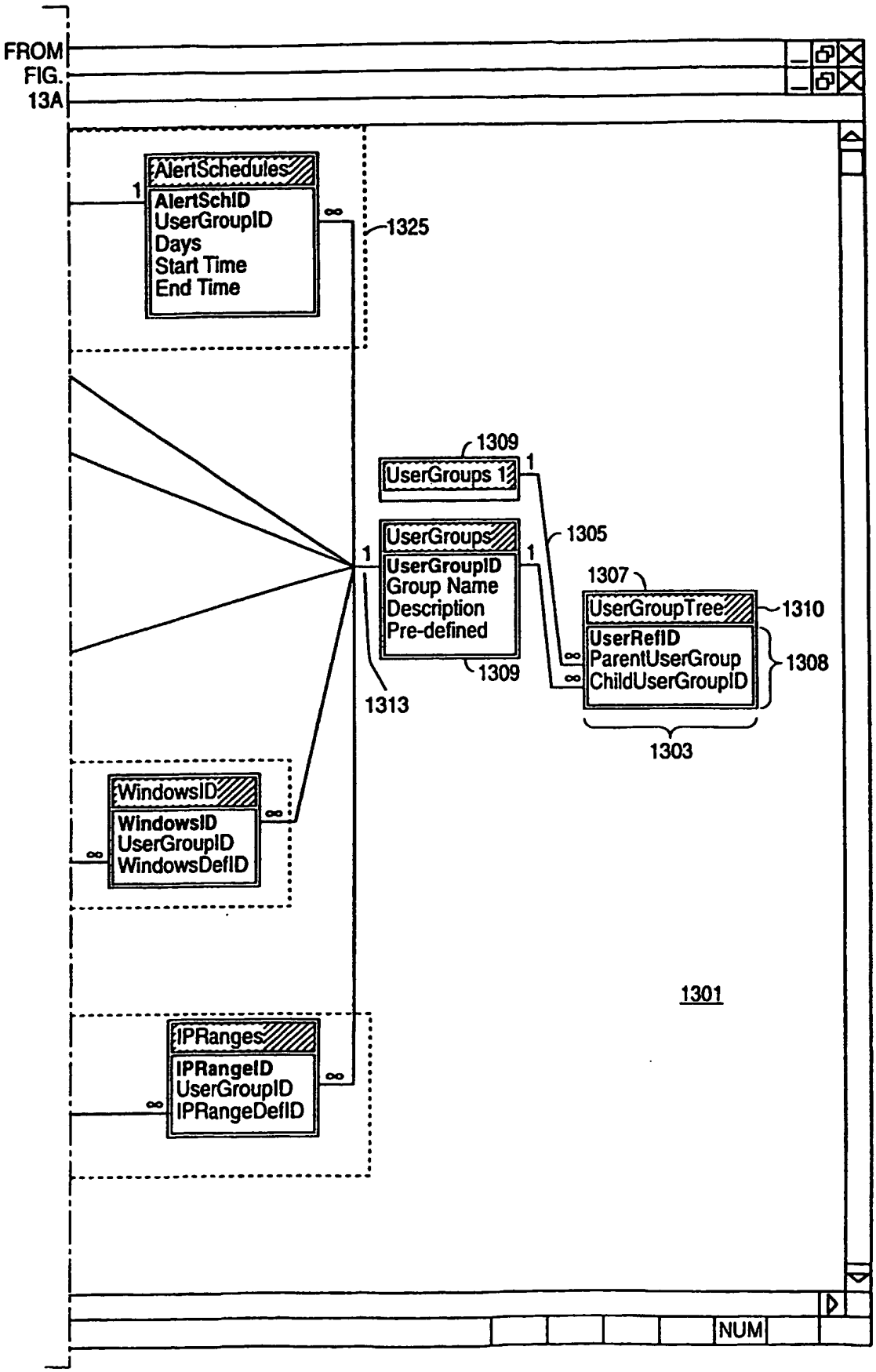

FROM FIG. 13A
AlertSchedules
AlertSchID
UserGroupID
Days
Start Time
End Time
1325
1309
UserGroups 1
UserGroups
UserGroupID
Group Name
Description
Pre-defined
1309
1305
1307
UserGroupTree
1310
UserRefID
ParentUserGroup
ChildUserGroupID
1308
1303
1313
WindowsID
WindowsID
UserGroupID
WindowsDefID
1301
IPRanges
IPRangeID
UserGroupID
IPRangeDefID
NUM

Fig. 13B

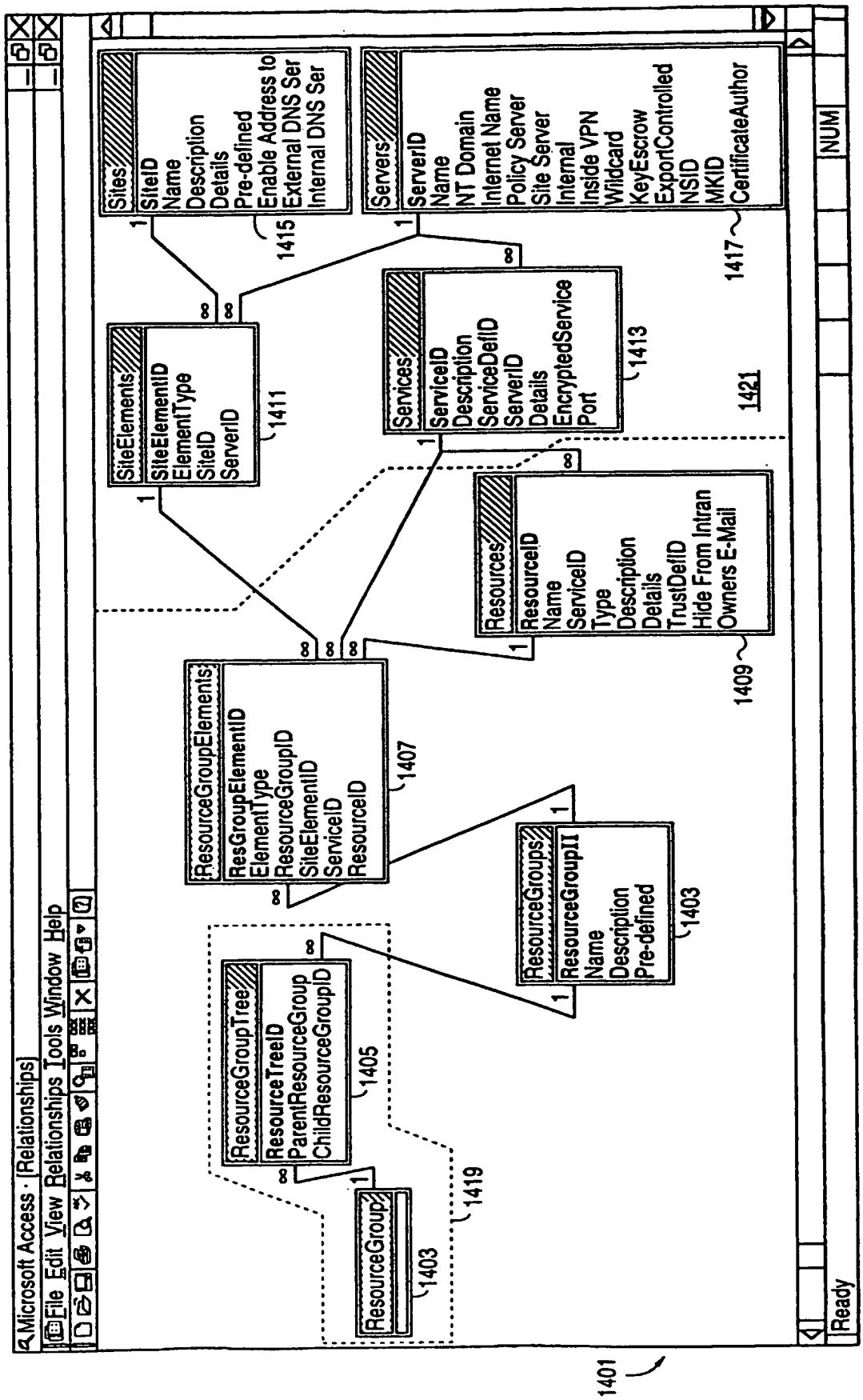

Microsoft Access - [Relationships]
File Edit View Relationships Tools Window Help
Sites
SiteID
Name
Description
Details
Pre-defined
Enable Address to
External DNS Ser
Internal DNS Ser
1415
Servers
ServerID
Name
NT Domain
Internet Name
Policy Server
Site Server
Internal
Inside VPN
Wildcard
KeyEscrow
ExportControlled
NSID
MKID
CertificateAuthor
1417
SiteElements
SiteElementID
ElementType
SiteID
ServerID
1411
Services
ServiceID
Description
ServiceDefID
ServerID
Details
EncryptedService
Port
1413
1421
Resources
ResourceID
Name
ServiceID
Type
Description
Details
TrustDefID
Hide From Intran
Owners E-Mail
1409
ResourceGroupElements
ResGroupElementID
ElementType
ResourceGroupID
SiteElementID
ServiceID
ResourceID
1407
ResourceGroups
ResourceGroupII
Name
Description
Pre-defined
1403
ResourceGroupTree
ResourceTreeID
ParentResourceGroup
ChildResourceGroupID
1405
ResourceGroup
1403
1419
NUM
Ready
1401

Fig. 14

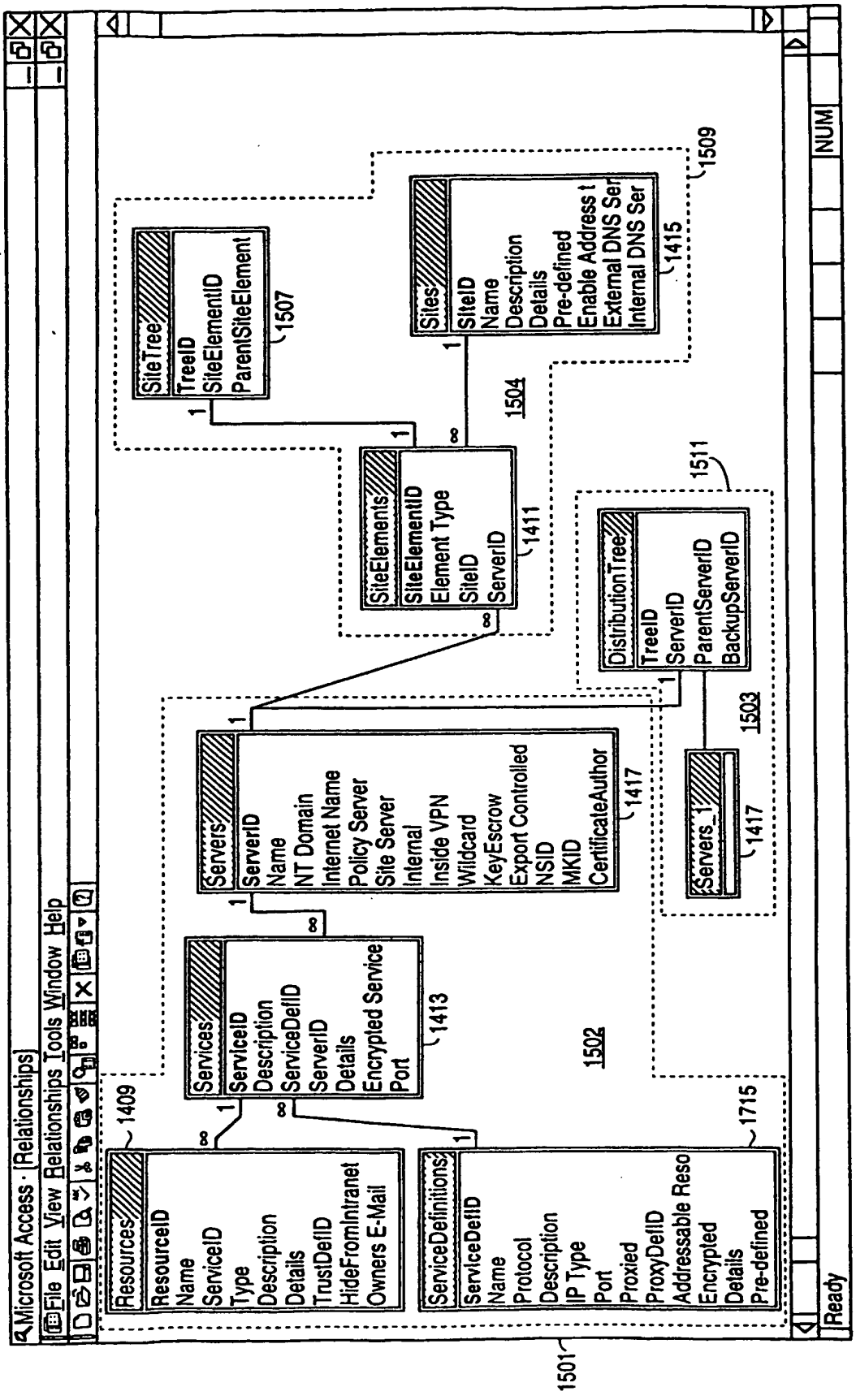

Microsoft Access - [Relationships]
File Edit View Relationships Tools Window Help
Ready
NUM
SiteTree
TreeID
SiteElementID
ParentSiteElement
1507
Sites
SiteID
Name
Description
Details
Pre-defined
Enable Address t
External DNS Ser
Internal DNS Ser
1415
1509
1504
SiteElements
SiteElementID
Element Type
SiteID
ServerID
1411
1511
DistributionTree
TreeID
ServerID
ParentServerID
BackupServerID
1503
Servers
ServerID
Name
NT Domain
Internet Name
Policy Server
Site Server
Internal
Inside VPN
Wildcard
KeyEscrow
Export Controlled
NSID
MKID
CertificateAuthor
1417
Servers_1
1417
Services
ServiceID
Description
ServiceDefID
ServerID
Details
Encrypted Service
Port
1413
1502
Resources
ResourceID
Name
ServiceID
Type
Description
Details
TrustDefID
HideFromIntranet
Owners E-Mail
1409
ServiceDefinitions
ServiceDefID
Name
Protocol
Description
IP Type
Port
Proxied
ProxyDefID
Addressable Reso
Encrypted
Details
Pre-defined
1715
1501

Fig. 15

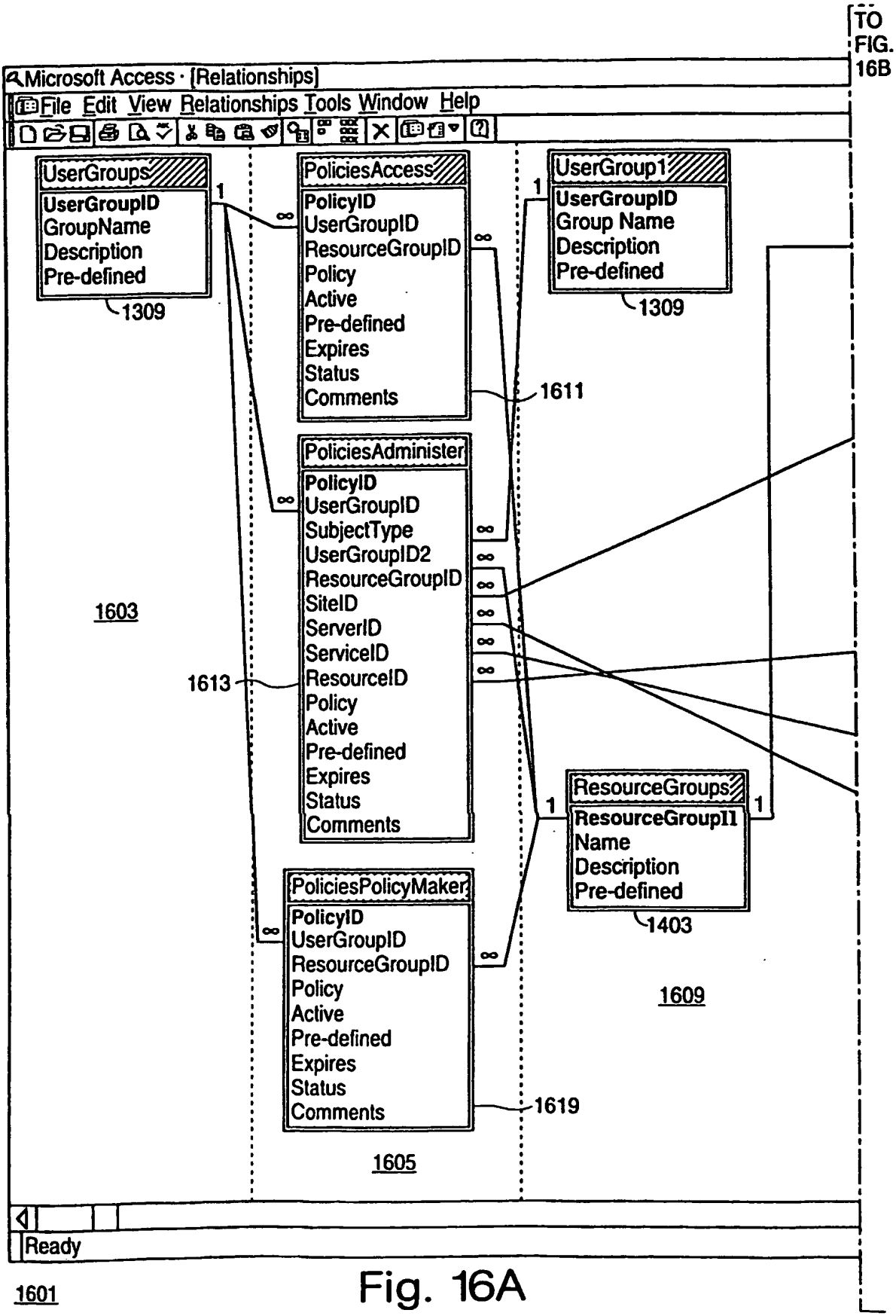

TO FIG. 16B
Microsoft Access - [Relationships]
File Edit View Relationships Tools Window Help
UserGroups
UserGroupID
GroupName
Description
Pre-defined
1309
PoliciesAccess
PolicyID
UserGroupID
ResourceGroupID
Policy
Active
Pre-defined
Expires
Status
Comments
1611
UserGroup1
UserGroupID
Group Name
Description
Pre-defined
1309
PoliciesAdminister
PolicyID
UserGroupID
SubjectType
UserGroupID2
ResourceGroupID
SiteID
ServerID
ServiceID
ResourceID
Policy
Active
Pre-defined
Expires
Status
Comments
1603
1613
ResourceGroups
ResourceGroupI1
Name
Description
Pre-defined
1403
1609
PoliciesPolicyMaker
PolicyID
UserGroupID
ResourceGroupID
Policy
Active
Pre-defined
Expires
Status
Comments
1619
1605
Ready
1601

Fig. 16A

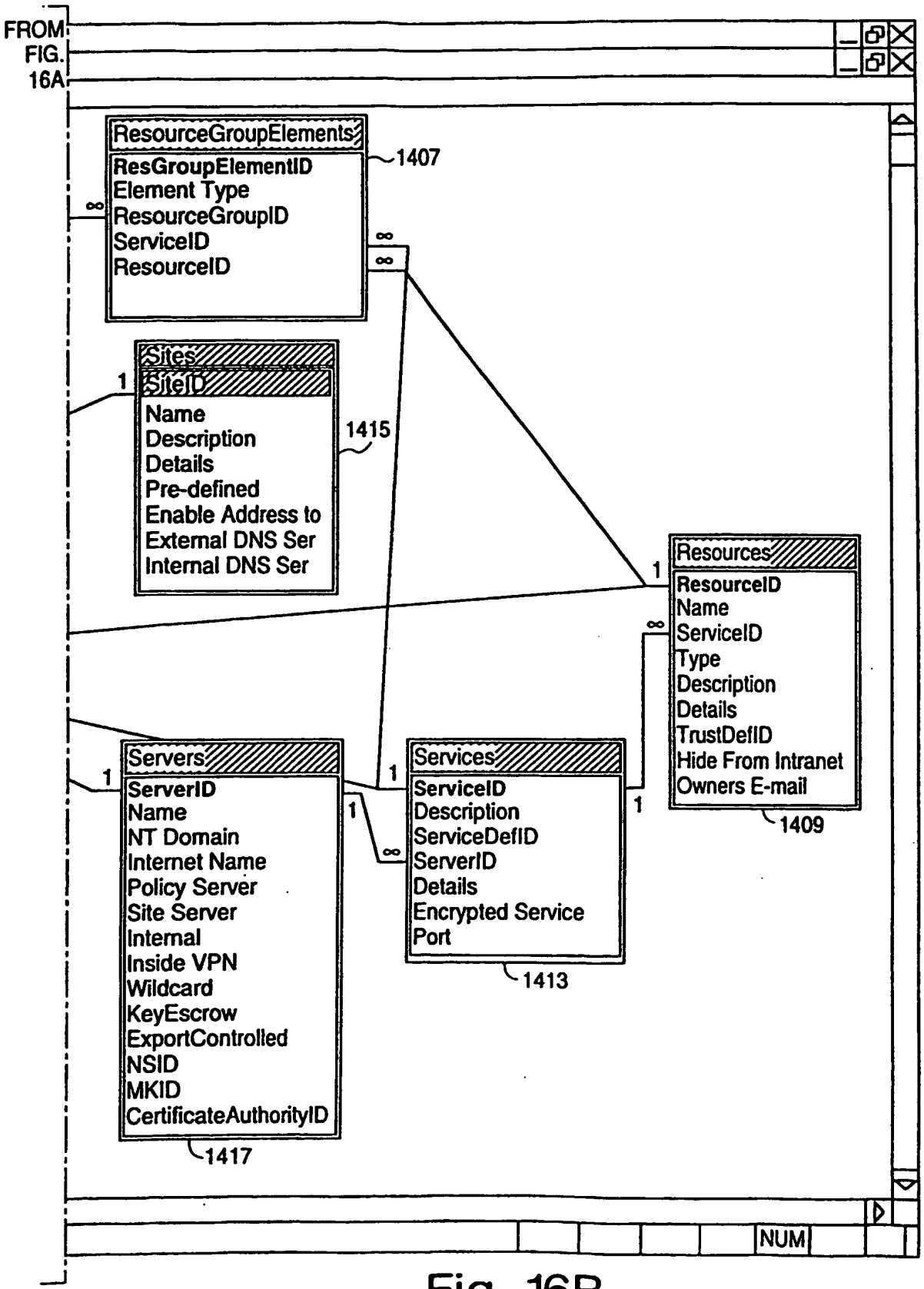

FROM FIG. 16A
ResourceGroupElements
ResGroupElementID
Element Type
ResourceGroupID
ServiceID
ResourceID
1407
Sites
SiteID
Name
Description
Details
Pre-defined
Enable Address to
External DNS Ser
Internal DNS Ser
1415
Resources
ResourceID
Name
ServiceID
Type
Description
Details
TrustDefID
Hide From Intranet
Owners E-mail
1409
Servers
ServerID
Name
NT Domain
Internet Name
Policy Server
Site Server
Internal
Inside VPN
Wildcard
KeyEscrow
ExportControlled
NSID
MKID
CertificateAuthorityID
1417
Services
ServiceID
Description
ServiceDefID
ServerID
Details
Encrypted Service
Port
1413
NUM

Fig. 16B

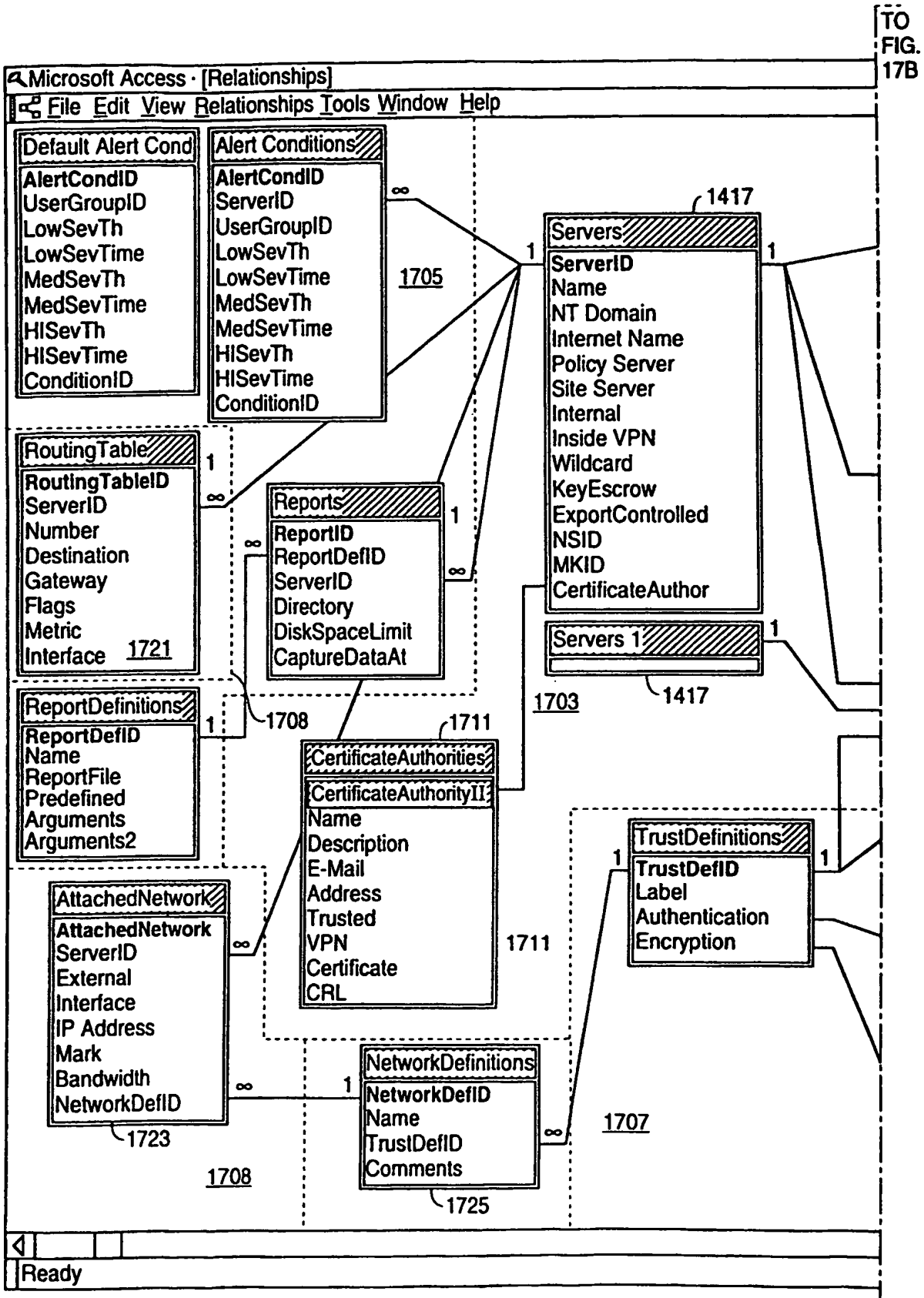

TO FIG. 17B
Microsoft Access - [Relationships]
File Edit View Relationships Tools Window Help
Default Alert Cond
AlertCondID
UserGroupID
LowSevTh
LowSevTime
MedSevTh
MedSevTime
HISevTh
HISevTime
ConditionID
Alert Conditions
AlertCondID
ServerID
UserGroupID
LowSevTh
LowSevTime
MedSevTh
MedSevTime
HISevTh
HISevTime
ConditionID
1705
1417
Servers
ServerID
Name
NT Domain
Internet Name
Policy Server
Site Server
Internal
Inside VPN
Wildcard
KeyEscrow
ExportControlled
NSID
MKID
CertificateAuthor
RoutingTable
RoutingTableID
ServerID
Number
Destination
Gateway
Flags
Metric
Interface
1721
Reports
ReportID
ReportDefID
ServerID
Directory
DiskSpaceLimit
CaptureDataAt
Servers 1
1417
1703
ReportDefinitions
ReportDefID
Name
ReportFile
Predefined
Arguments
Arguments2
1708
1711
CertificateAuthorities
CertificateAuthorityII
Name
Description
E-Mail
Address
Trusted
VPN
Certificate
CRL
1711
TrustDefinitions
TrustDefID
Label
Authentication
Encryption
AttachedNetwork
AttachedNetwork
ServerID
External
Interface
IP Address
Mark
Bandwidth
NetworkDefID
1723
NetworkDefinitions
NetworkDefID
Name
TrustDefID
Comments
1725
1707
1708
Ready
701

Fig. 17A

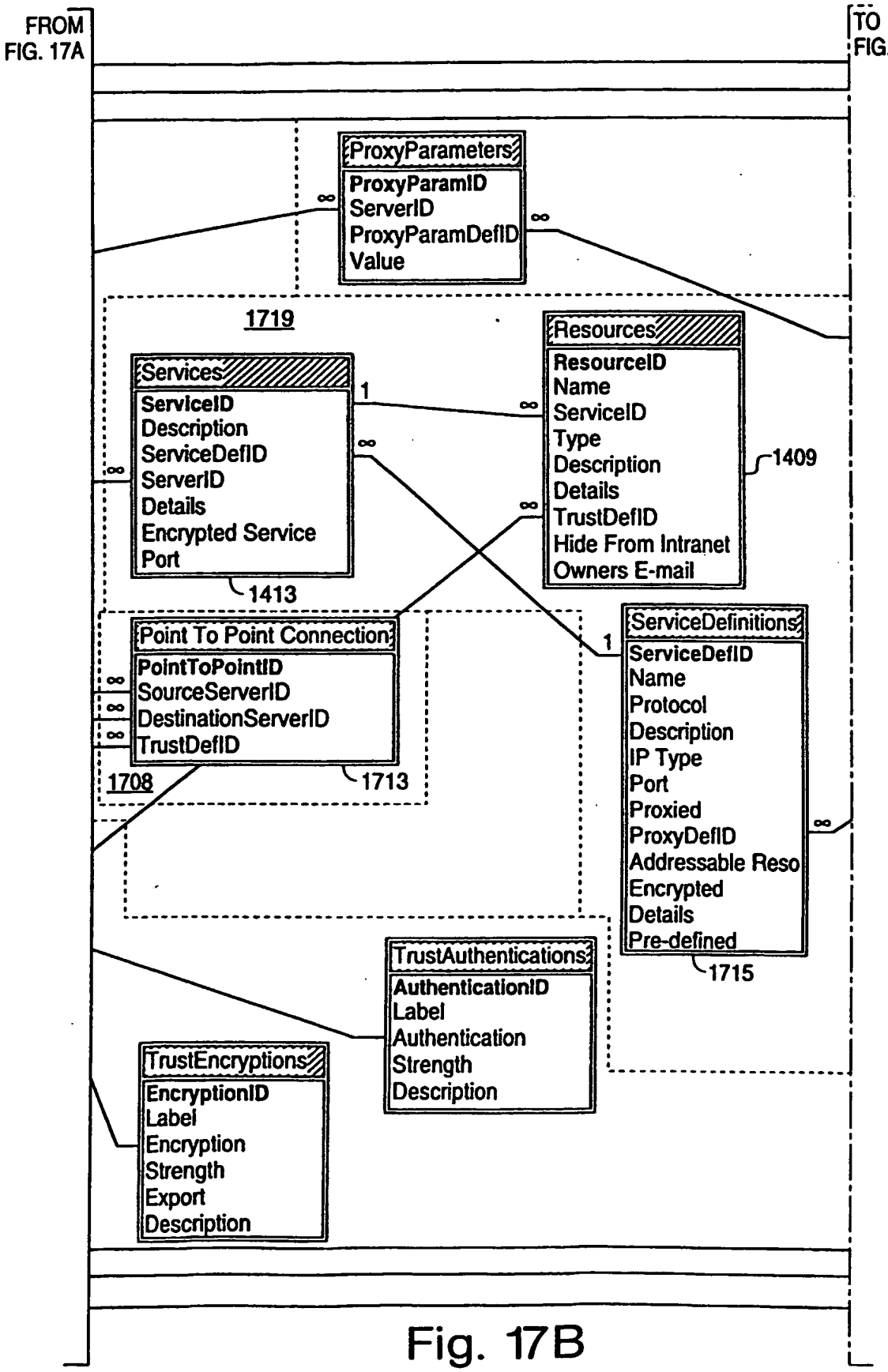

FROM FIG. 17A
TO FIG. 17C
ProxyParameters
ProxyParamID
ServerID
ProxyParamDefID
Value
1719
Services
ServiceID
Description
ServiceDefID
ServerID
Details
Encrypted Service
Port
1413
Resources
ResourceID
Name
ServiceID
Type
Description
Details
TrustDefID
Hide From Intranet
Owners E-mail
1409
Point To Point Connection
PointToPointID
SourceServerID
DestinationServerID
TrustDefID
1708
1713
ServiceDefinitions
ServiceDefID
Name
Protocol
Description
IP Type
Port
Proxied
ProxyDefID
Addressable Reso
Encrypted
Details
Pre-defined
1715
TrustAuthentications
AuthenticationID
Label
Authentication
Strength
Description
TrustEncryptions
EncryptionID
Label
Encryption
Strength
Export
Description

Fig. 17B

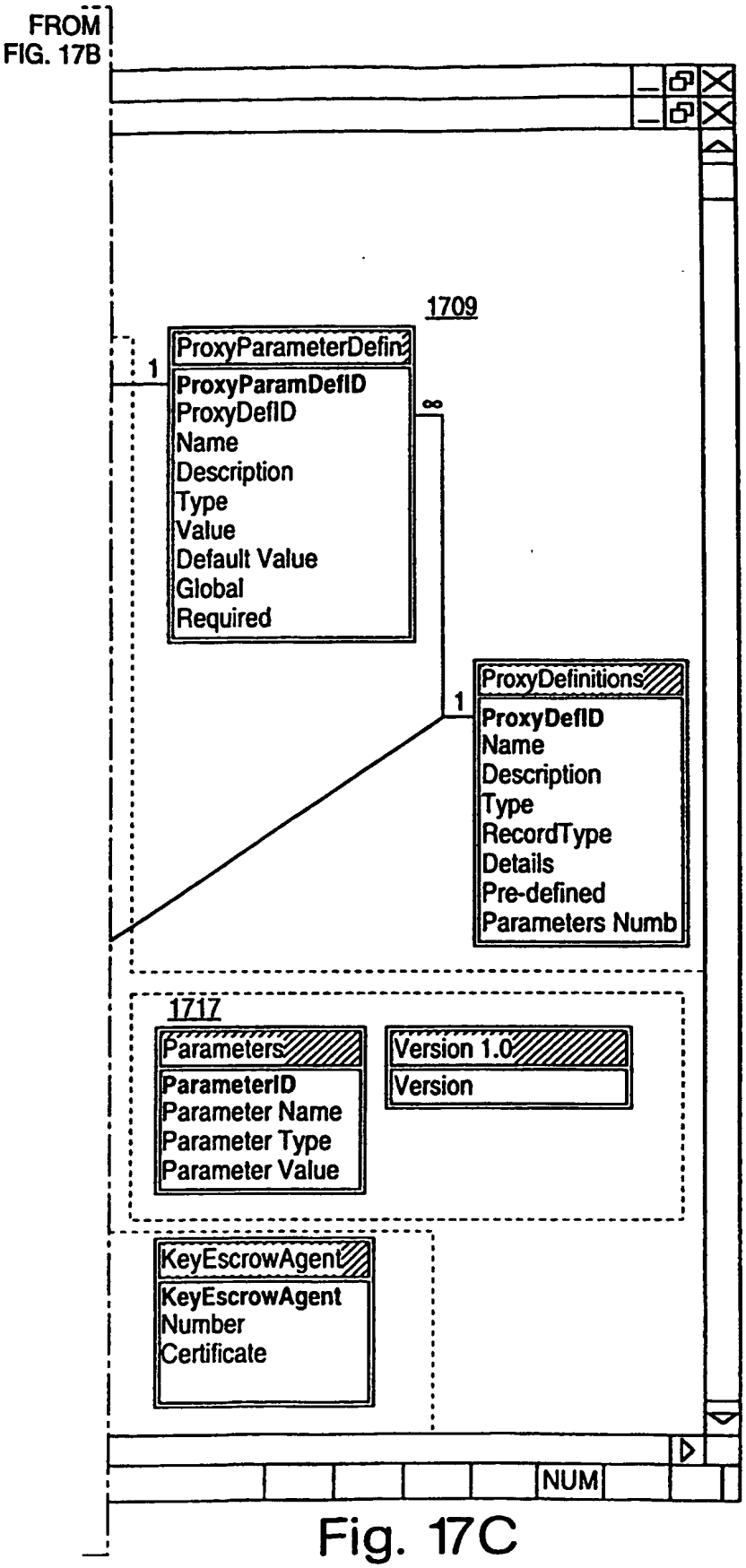

FROM FIG. 17B
1709
ProxyParameterDefin
ProxyParamDefID
ProxyDefID
Name
Description
Type
Value
Default Value
Global
Required
1
∞
ProxyDefinitions
ProxyDefID
Name
Description
Type
RecordType
Details
Pre-defined
Parameters Numb
1717
Parameters
ParameterID
Parameter Name
Parameter Type
Parameter Value
Version 1.0
Version
KeyEscrowAgent
KeyEscrowAgent Number
Certificate
NUM

Fig. 17C

Docket Proof

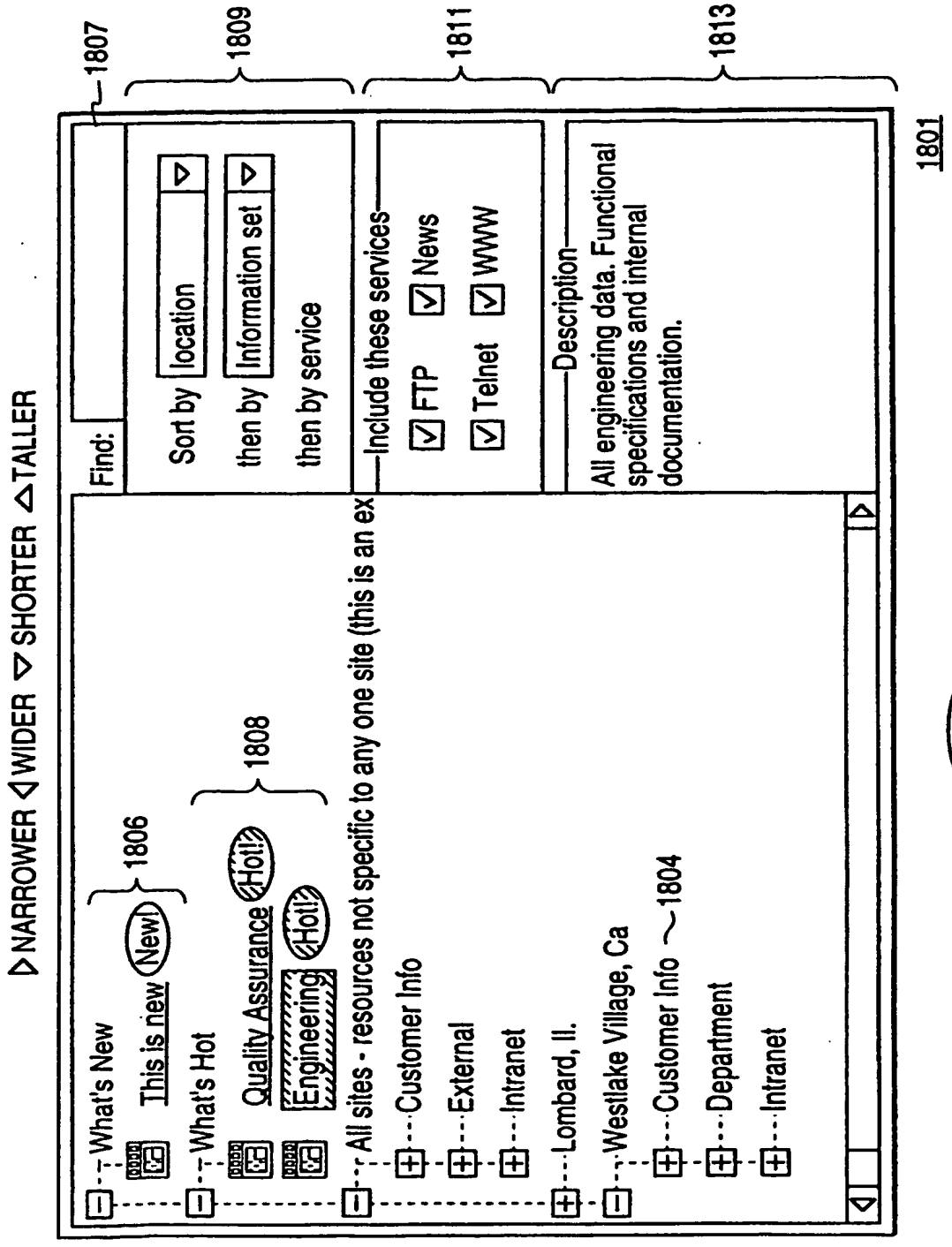


Fig. 18

10/019101

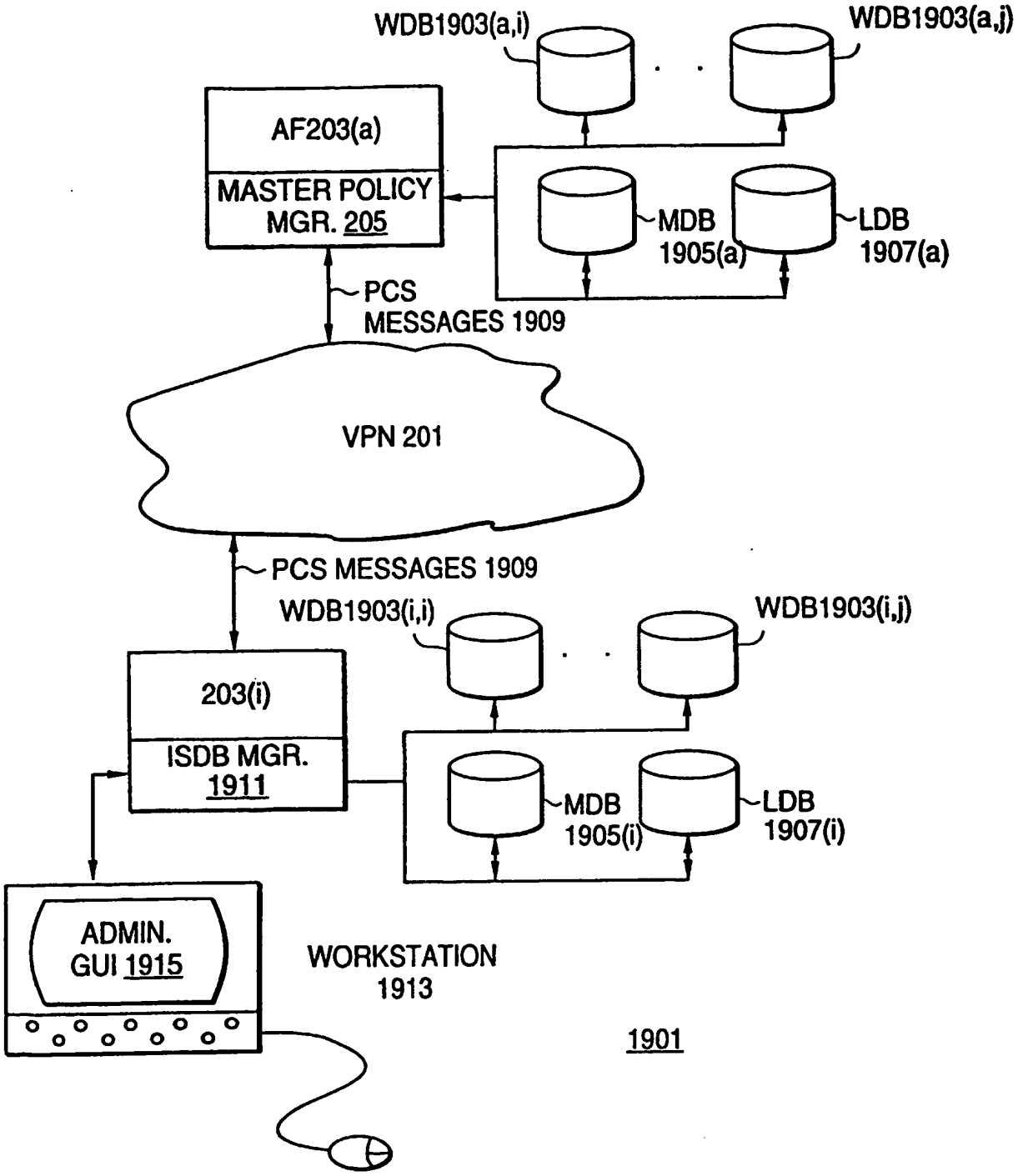


Fig. 19

10/021,101

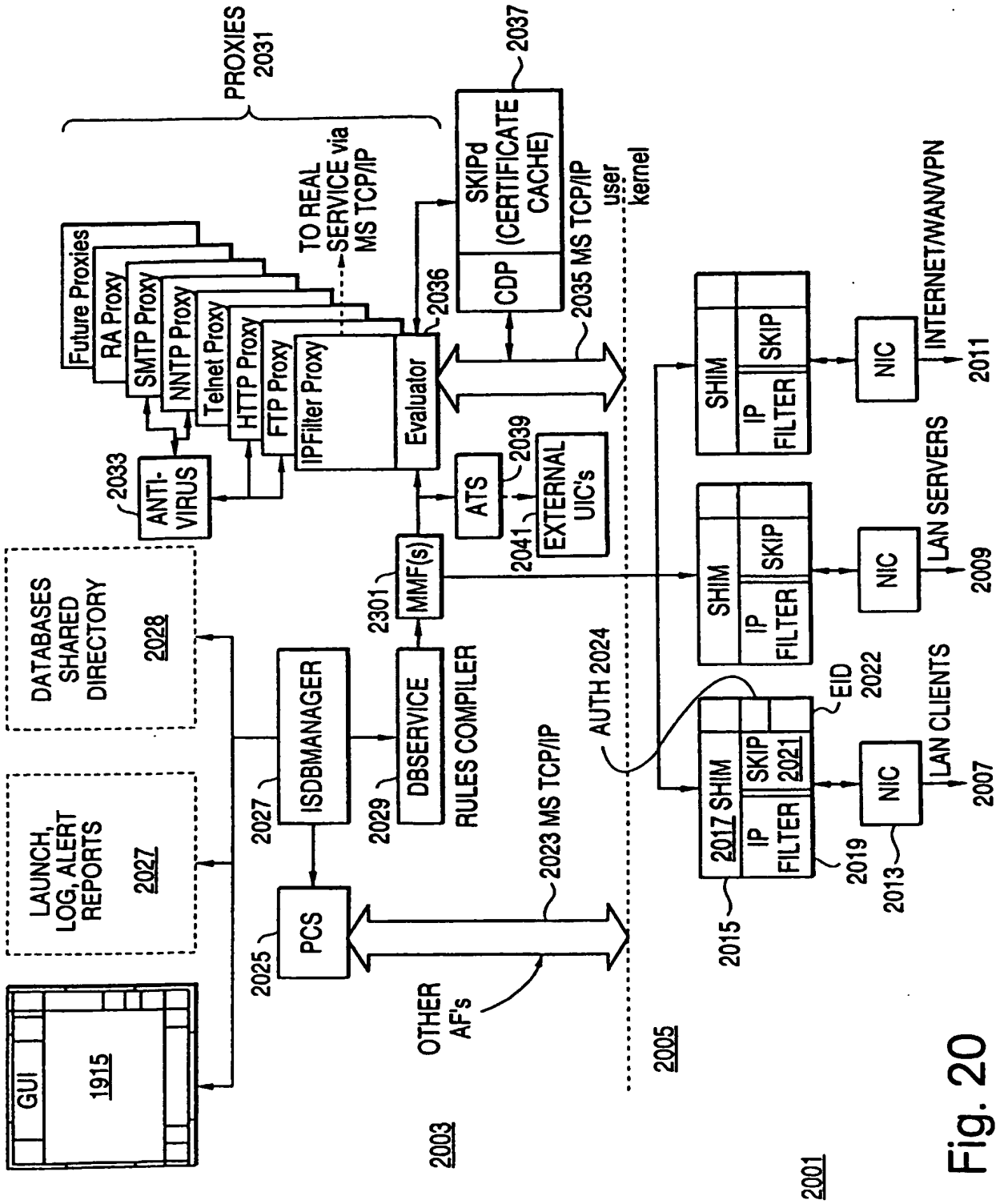


Fig. 20

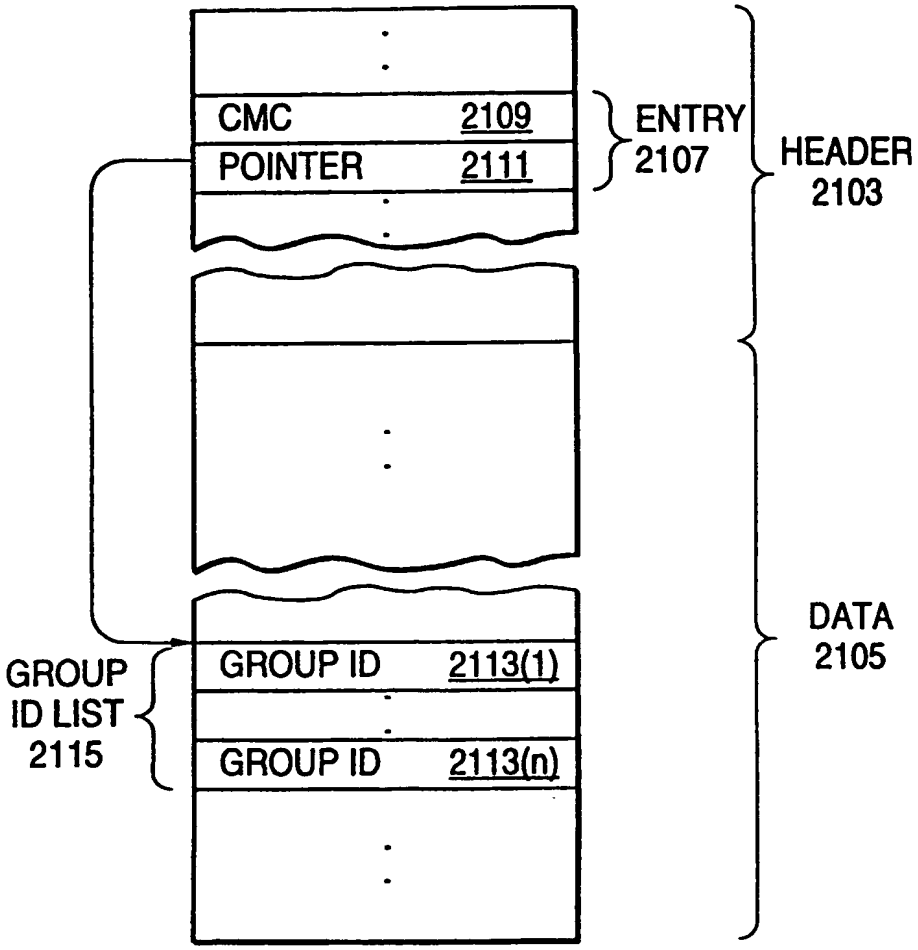

CMC 2109
POINTER 2111
ENTRY 2107
HEADER 2103
DATA 2105
GROUP ID LIST 2115
GROUP ID 2113(1)
GROUP ID 2113(n)
DB CERTIFICATES BY USER GROUP FILE 2101
2303

Fig. 21

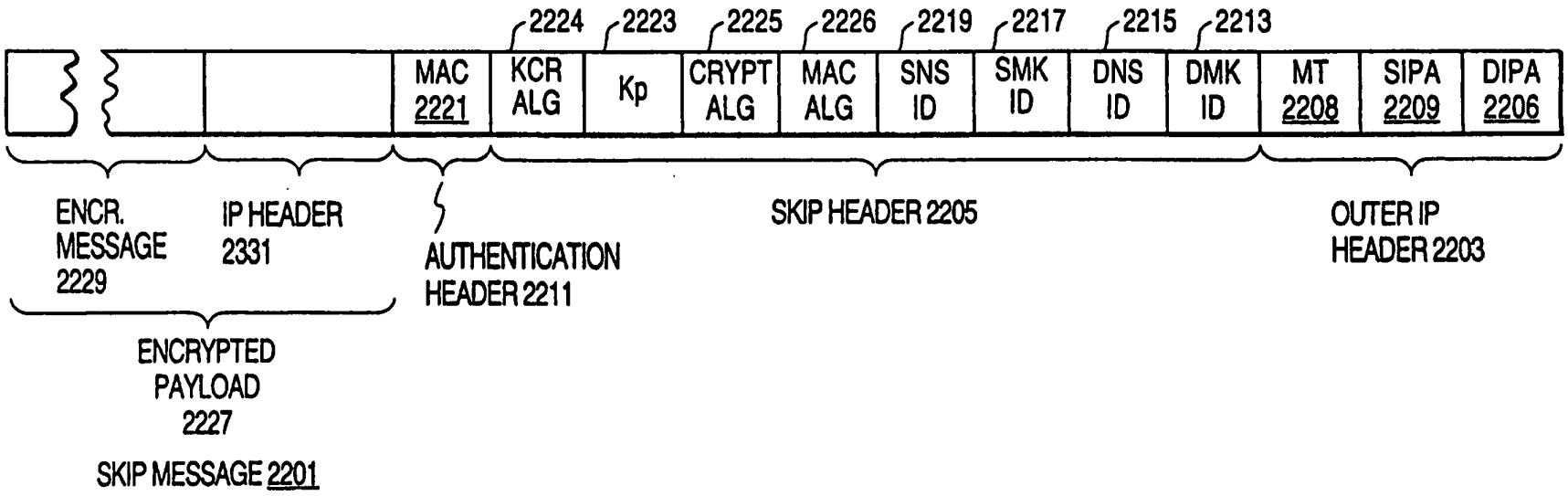

2224
2223
2225
2226
2219
2217
2215
2213
MAC 2221
KCR ALG
Kp
CRYPT ALG
MAC ALG
SNS ID
SMK ID
DNS ID
DMK ID
MT 2208
SIPA 2209
DIPA 2206
ENCR. MESSAGE 2229
IP HEADER 2331
AUTHENTICATION HEADER 2211
SKIP HEADER 2205
OUTER IP HEADER 2203
ENCRYPTED PAYLOAD 2227
SKIP MESSAGE 2201

Fig. 22

File 2303

MMF File Name	Contents
	Policies, User Groups, and Information Sets 2305
DBUsersFile 2307	Describes policy application from the User Group viewpoint. Maps each DB UserGroupID to a list of ResourceGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBUsersTreeFile	Describes the user groups tree as a flattened array. Maps each DB UserGroup ID to a list of UserGroupIDs for parent user groups
DBResourcesFile 2309	Describes policy application from the Resource Group (information set) viewpoint. Maps each DB ResourceGroupID to a list of UserGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBResourcesTreeFile	Describes the resource groups tree as a flattened array. Maps each DB ResourceGroupID to a list of ResourceGroupIDs for parent information sets.
	User Identification Information 2311
DBIPRangesFile	IP Ranges data. Maps from IPRangeDefID to the IP range data.
DBDomainsFile	IP Domain data. Maps from DomainDefID to the IP domain data.
DBCertificatesFile	Certificate data. Maps from CertificateDefID to the certificate data.
DBWindowsIDFile	Windows ID data. Maps from WindowDefID to the windows ID data.
DBSmartCardIDFile	Smart card (authentication token) data. Maps from SmartcardDefID to the authentication token data.
DBIPRangesByUserGroup File	Relates IP range matching criteria to user groups. Maps from IP Range data to UserGroupIDs.
DBDomainsByUserGroup File	Relates IP domain matching criteria to user groups. Maps from IP Domain data to UserGroupIDs.
DBCertificatesByUserGroup File	Relates certificates to user groups. Maps from certificate data to UserGroupIDs. 2101
DBWindowsIDByUserGroup File	Relates Windows IDs to user groups. Maps from Windows ID data to UserGroupIDs.
DBSmartCardIDByUser GroupFile	Relates Smart Card (authentication token) data to user groups. Maps from authentication token data to UserGroupIDs

2301

Fig. 23A

MMF File Name	Contents
	Servers, Services, and Information Resources 2313
DBResourcesByServerIDFile	Relates servers to resources. Maps from ServerIDs to ResourceIDs for resources held on the server identified by the ServerID.
DBResourcesByServiceIDFile	Relates services to resources. Maps from ServiceIDs to ResourceIDs for resources belonging to the service identified by the ServiceID.
DBResourceIDByServiceIDFile	Relates services to their information resources. Maps from ServiceID to ResourceID.
DBResourceIDByNameFile 2315	Relates the IP names (URLs) of resources to resource IDs. Maps from URL to resource ID.
DBResourcesByResourceIDFile 2317	Relates resources to information sets. Maps ResourceID to Resource GroupIds.
	Servers, Services, IP Information, and Proxies 2319
DBServerIDByIPFile	Relates IP addresses to servers. Maps IP addresses to ServerIDs.
DBServerIDByNameFile	Relates IP names to servers. Maps the IP FQDN (fully qualified domain name) for each server to its ServerID.
DBIPAndTypeByServerIDFile	Relates servers to their locations inside or outside to the VPN. Maps ServerID to the server's IP address and a flag indicating whether the address is inside or outside the VPN.
DBServiceIDByPortFile	Relates services to their port numbers. Maps from ServiceID to port number.
DBServiceIDByServerIDFile	Relates servers to ports for services. Maps from ServerID to a list of port numbers.
DBServicePortToProxyPortFile	Relates service ports to the ports for their proxies. Maps from service port number to proxy port number.
DBProxyIDByServerIDFile	Relates servers to service proxies. Maps from ServerID to ProxyDefID.
DBProxyParametersFile	Relates proxies to configuration data for the proxies. Maps from ProxyDefID to options data

2301

Fig. 23B

MMF File Name	Contents
	Access Filter Information 2321
DBAttachedNetworksByIPFile	Relates network interfaces in the access filters to information for the interfaces. Maps from the interface's IP address to interface information.
DBAttachedNetworksByServerIDFile	Relates access filters to their network interfaces. Maps from ServerID for the access filter to interface information.
DBRoutingTableFile	Describes the IP routing information for all of the access filters. One block of information.
DBRoutingTableByServerIDFile	Relates access filters to their IP routing information. Maps from ServerID for the access filter to IP routing information.
DBPointToPointFile	Relates a point-to-point description of a network path to data for the path. Maps from PointToPointID for the path to the associated data.
	SEND Information 2323
DBTrustTableFile 2325	Implements the SEND table. Maps from TrustDefID, indicating a trust level, to AuthenticationIDs for user identification techniques and EncryptionIDs for encryption techniques.
DBCertificateAuthoritiesFile	Relates identifiers for cerfiticate authorities to their data. Maps from CertificateAuthorityID to associated data.
DBTrustAuthenticationsFile	Relates AuthenticationIDs to information about identification techniques. Maps from AuthenticationID to identification technique information.
DBTrustEncryptionsFile	Relates EncryptionIDs to information about encryption techniques. Maps from EncryptionID to encryption type and strength information.
	IntraMap Information 2422
DBJavaSiteTable	Maps from names of locations to LocationIDs.
DBJavaResourceTable	Maps from URLs of resources to their ResourceIDs, LocationIDs, and *hidden* flags.
DBJavaResourcesSetTable	Maps from names of information sets to ResourceGroupIDs, a list of ResourceIDs for all resources contained in the information set, and a list of ResourceGroupsIDs for all of the information set's parents.

2301

Fig. 23C

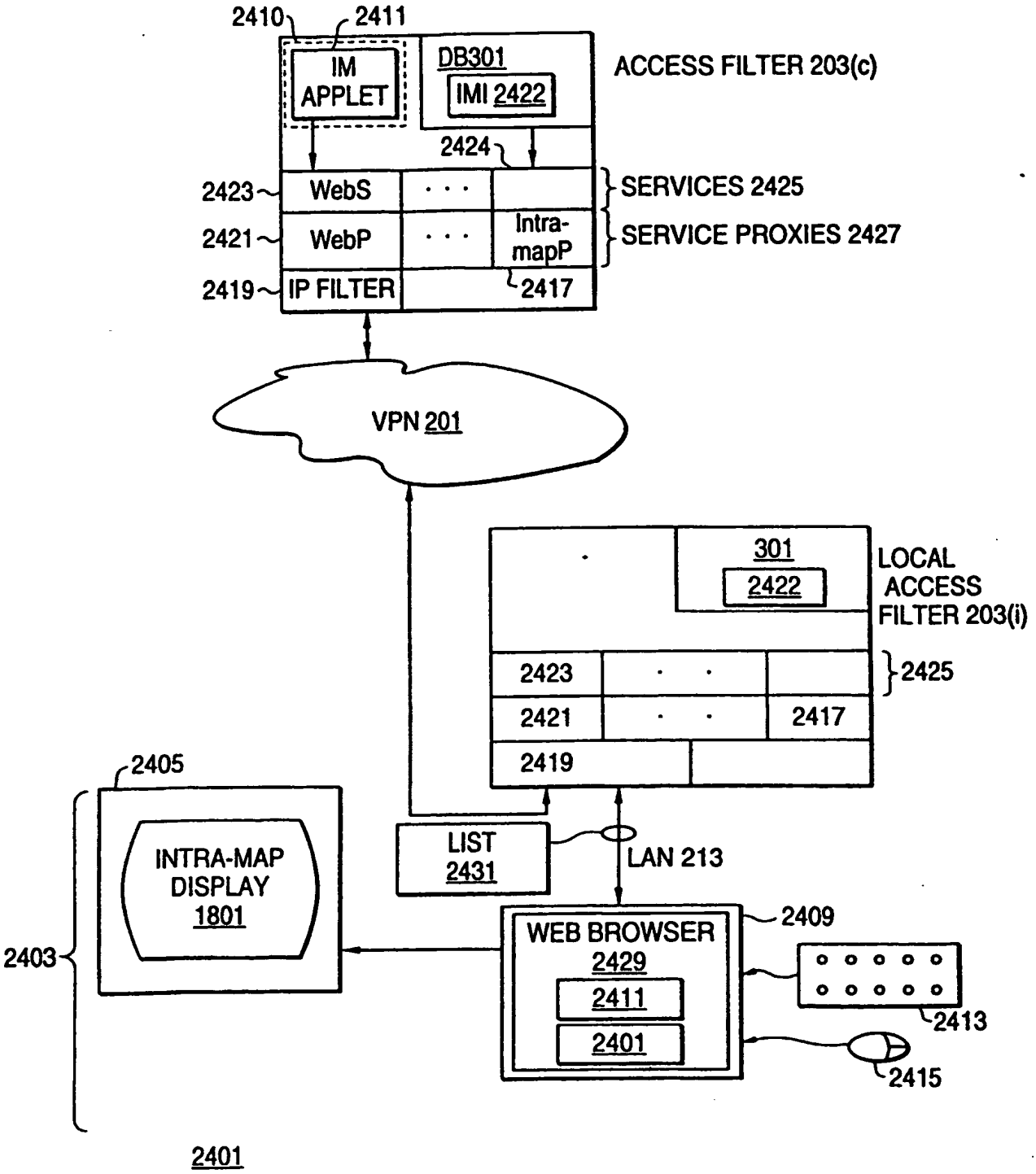

2410
2411
IM APPLET
DB301
IMI 2422
ACCESS FILTER 203(c)
2424
2423
WebS
SERVICES 2425
2421
WebP
Intra-mapP
SERVICE PROXIES 2427
2419
IP FILTER
2417
VPN 201
301
2422
LOCAL ACCESS FILTER 203(i)
2423
2425
2421
2417
2419
2405
INTRA-MAP DISPLAY 1801
LIST 2431
LAN 213
2409
WEB BROWSER 2429
2411
2401
2413
2415
2403
2401

Fig. 24

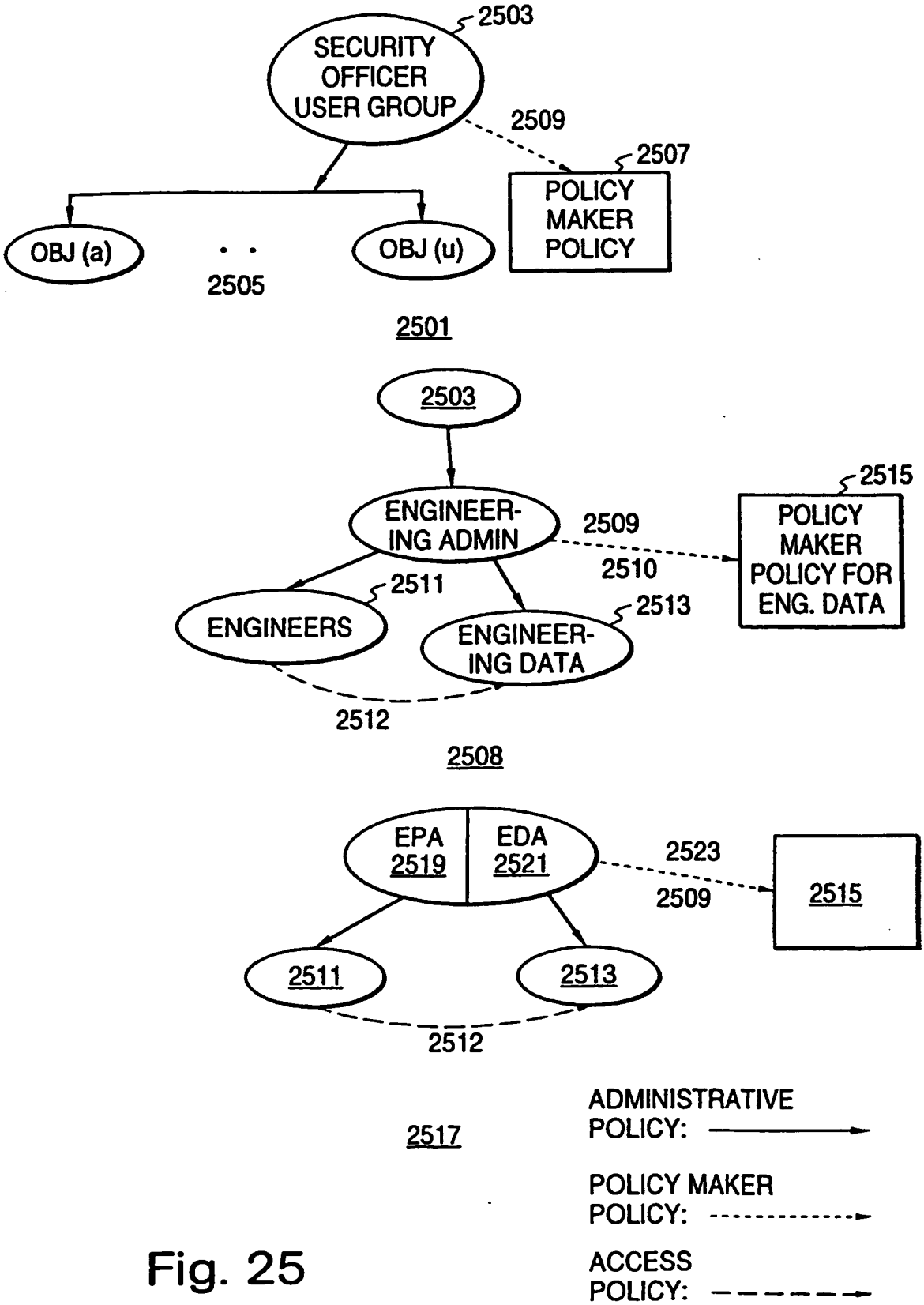

2503
SECURITY OFFICER USER GROUP
2509
2507
POLICY MAKER POLICY
OBJ (a)
OBJ (u)
2505
2501
2503
ENGINEER-ING ADMIN
2509
2510
2515
POLICY MAKER POLICY FOR ENG. DATA
2511
ENGINEERS
2513
ENGINEER-ING DATA
2512
2508
EPA 2519
EDA 2521
2523
2509
2515
2511
2513
2512
2517
ADMINISTRATIVE POLICY:
POLICY MAKER POLICY:
ACCESS POLICY:

Fig. 25

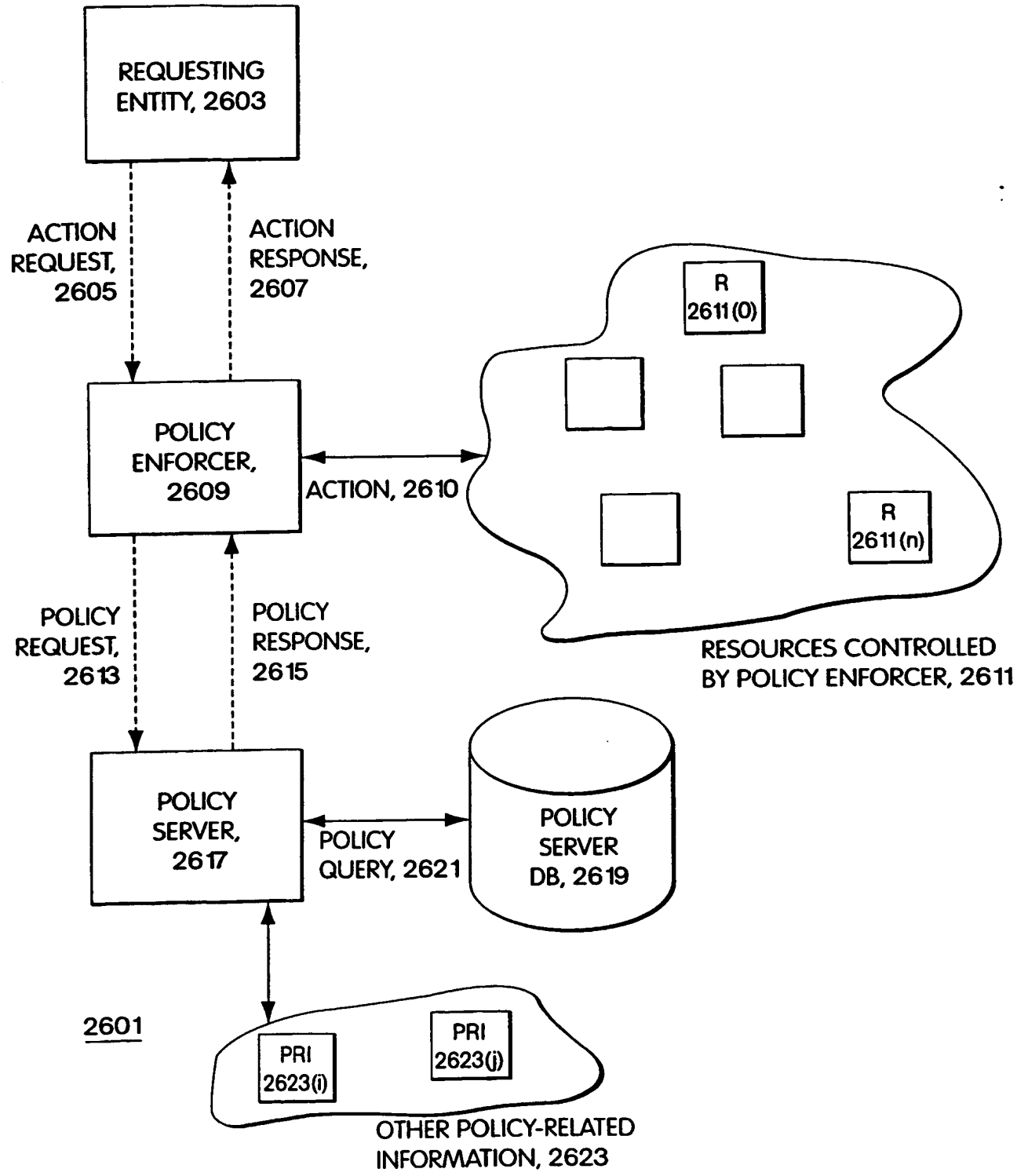

REQUESTING ENTITY, 2603
ACTION REQUEST, 2605
ACTION RESPONSE, 2607
POLICY ENFORCER, 2609
ACTION, 2610
R 2611(0)
R 2611(n)
RESOURCES CONTROLLED BY POLICY ENFORCER, 2611
POLICY REQUEST, 2613
POLICY RESPONSE, 2615
POLICY SERVER, 2617
POLICY QUERY, 2621
POLICY SERVER DB, 2619
2601
PRI 2623(i)
PRI 2623(j)
OTHER POLICY-RELATED INFORMATION, 2623

Fig. 26

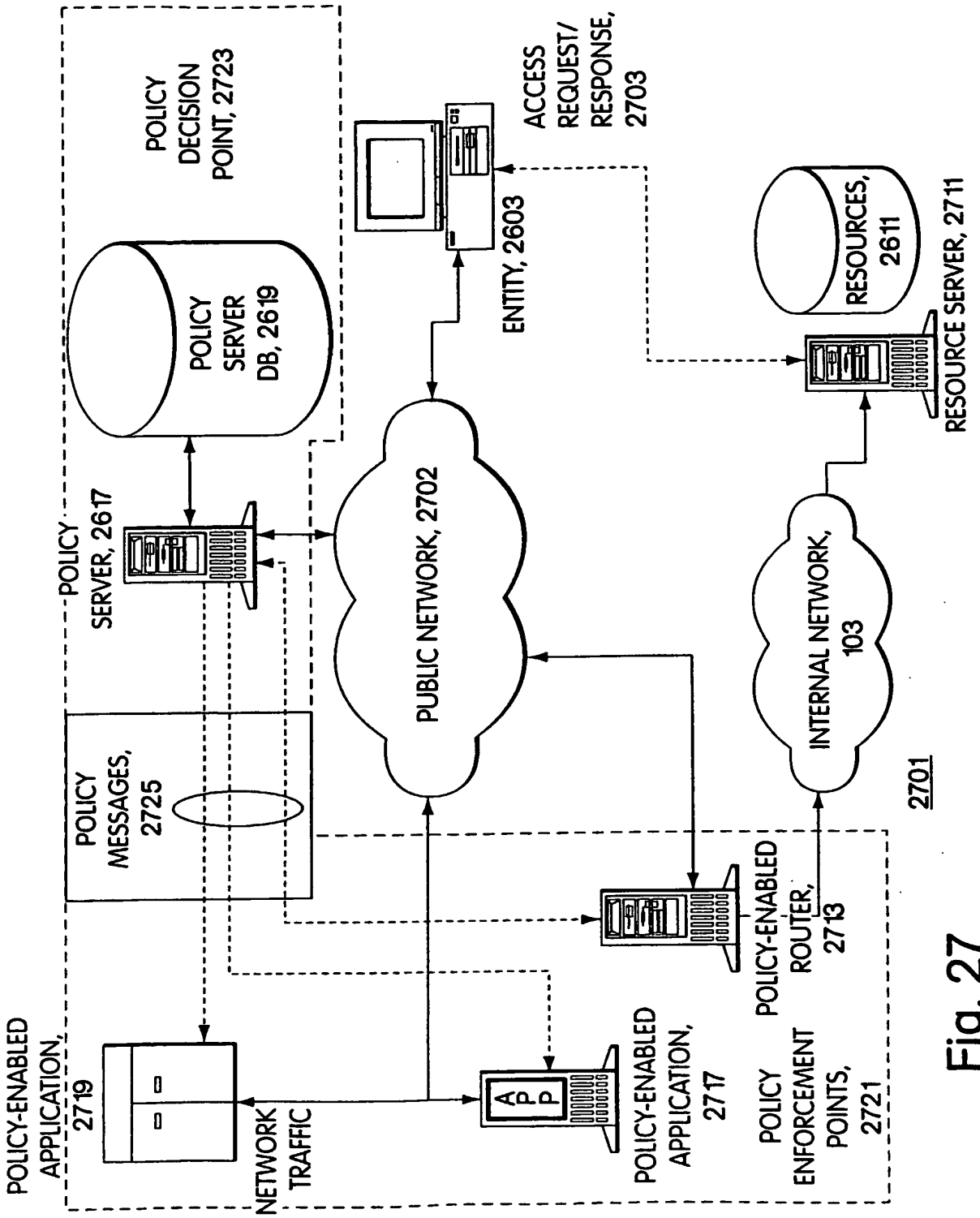

POLICY DECISION POINT, 2723
POLICY SERVER DB, 2619
POLICY SERVER, 2617
POLICY MESSAGES, 2725
POLICY-ENABLED APPLICATION, 2719
NETWORK TRAFFIC
PUBLIC NETWORK, 2702
ENTITY, 2603
ACCESS REQUEST/ RESPONSE, 2703
RESOURCES, 2611
RESOURCE SERVER, 2711
INTERNAL NETWORK, 103
POLICY-ENABLED ROUTER, 2713
POLICY-ENABLED APPLICATION, 2717
POLICY ENFORCEMENT POINTS, 2721
2701

Fig. 27

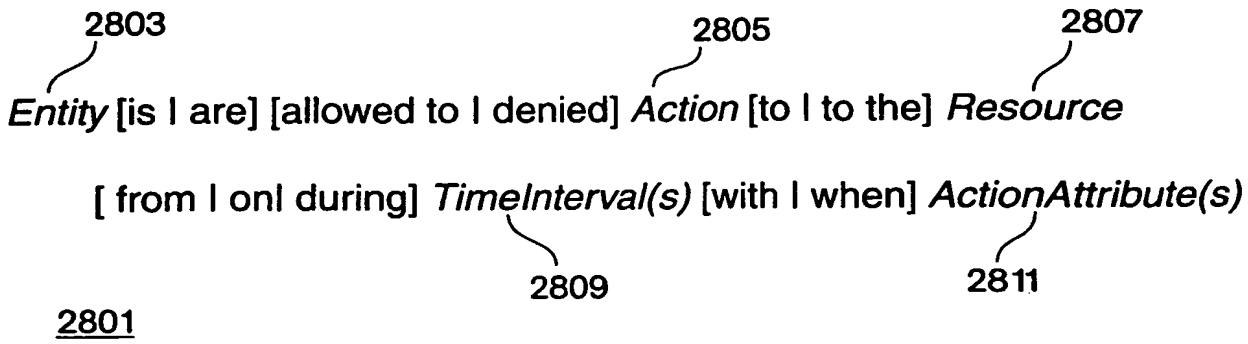


Fig. 28

SUBSTITUTE SHEET (RULE 26)

10/019101

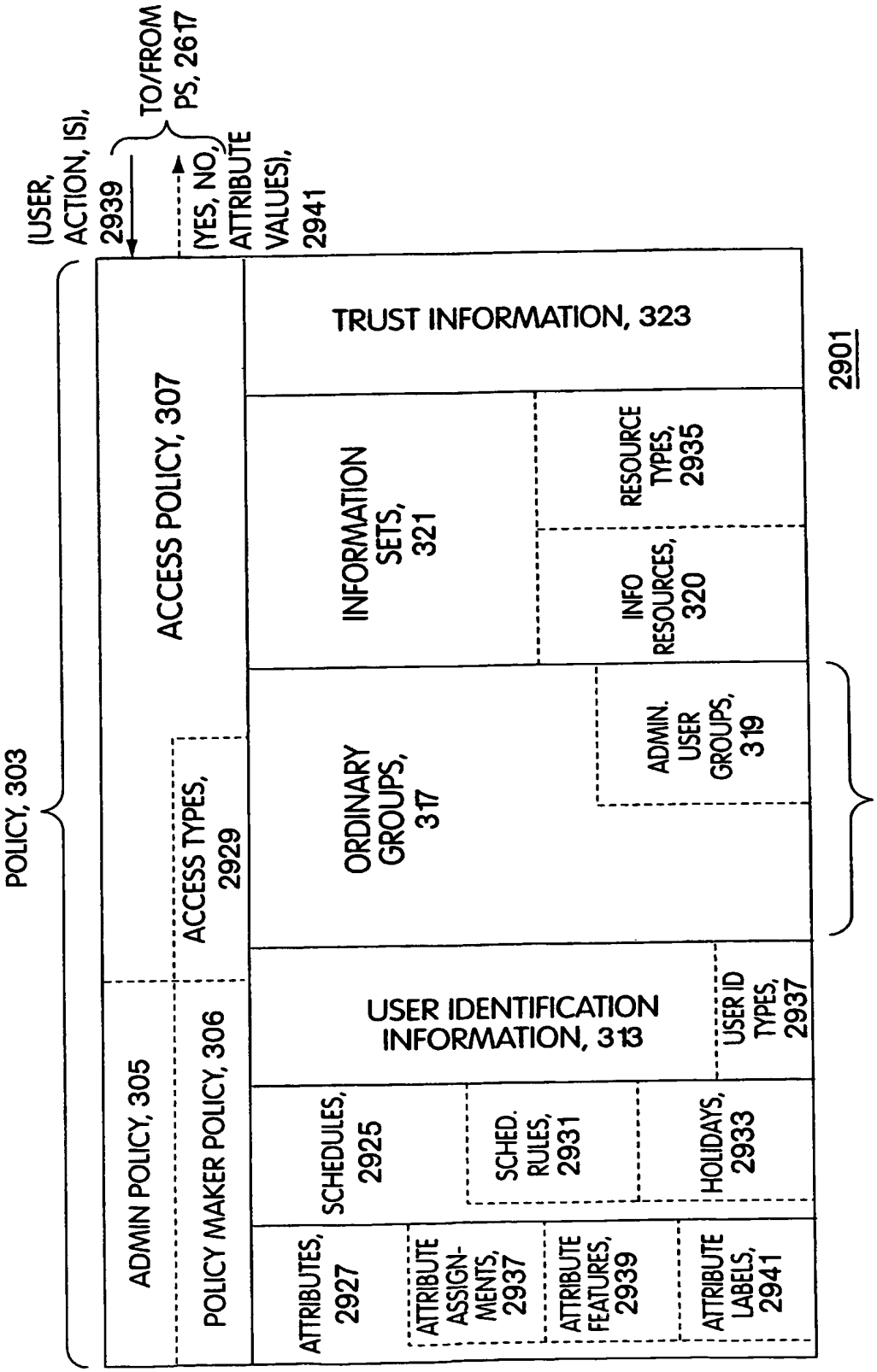


Fig. 29

10/019101

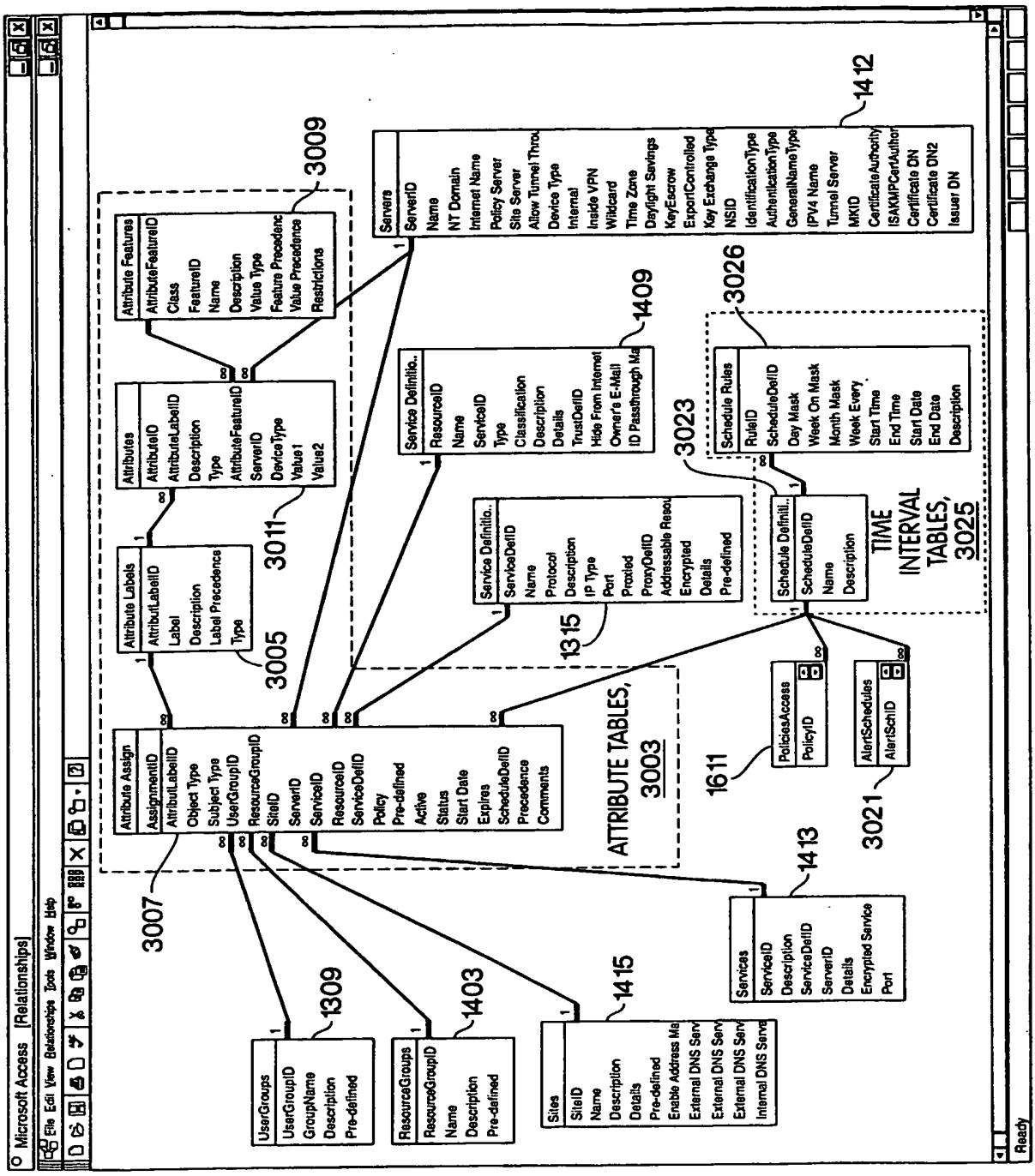


Fig. 30

3001

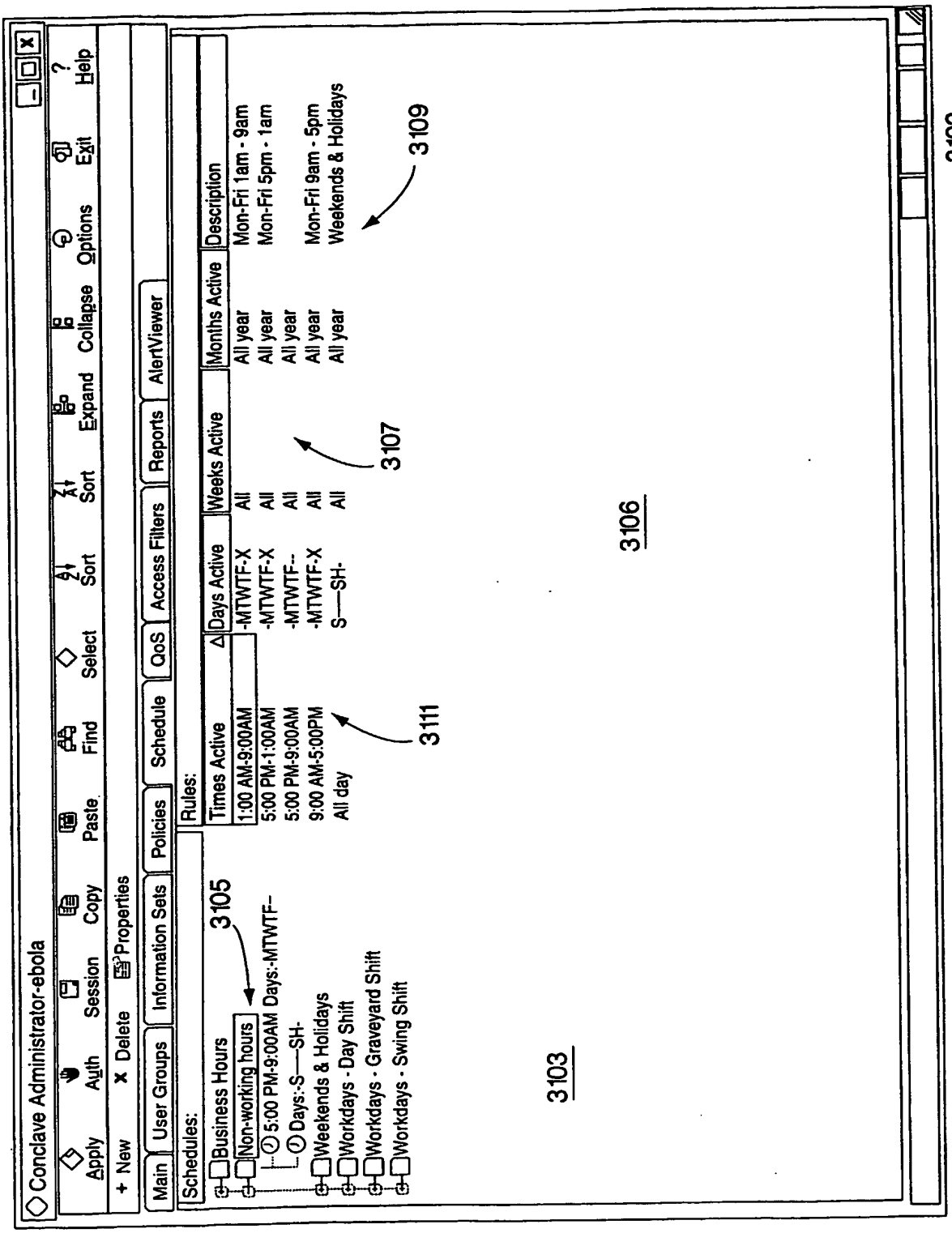

Conclave Administrator-ebola
Apply
Auth
Session
Copy
Paste
Find
Select
Sort
Sort
Expand
Collapse
Options
Exit
Help
+ New
Delete
Properties
Main
User Groups
Information Sets
Policies
Schedule
QoS
Access Filters
Reports
AlertViewer
Schedules:
Business Hours
Non-working hours
5:00 PM-9:00AM Days:-MTWTF-
Days:-S—SH-
Weekends & Holidays
Workdays - Day Shift
Workdays - Graveyard Shift
Workdays - Swing Shift
Rules:
Times Active
Days Active
Weeks Active
Months Active
Description
1:00 AM-9:00AM -MTWTF-X All All year Mon-Fri 1am - 9am
5:00 PM-1:00AM -MTWTF-X All All year Mon-Fri 5pm - 1am
5:00 PM-9:00AM -MTWTF-- All All year
9:00 AM-5:00PM -MTWTF-X All All year Mon-Fri 9am - 5pm
All day S—SH- All All year Weekends & Holidays
3105
3107
3109
3111
3103
3106
3102

Fig. 31

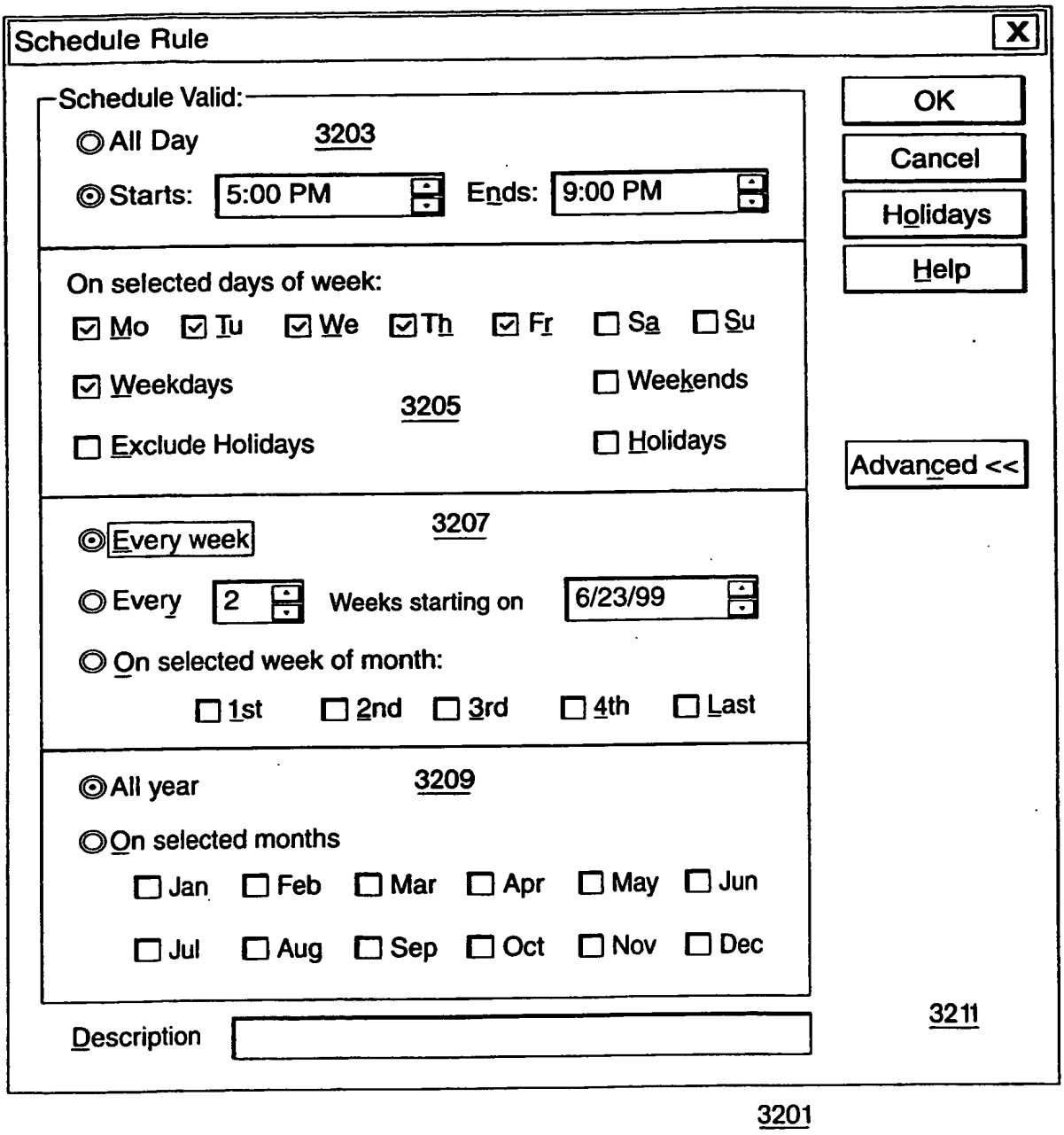


Fig. 32

FORM PCT/ISA/210 (second sheet) (July 1998)

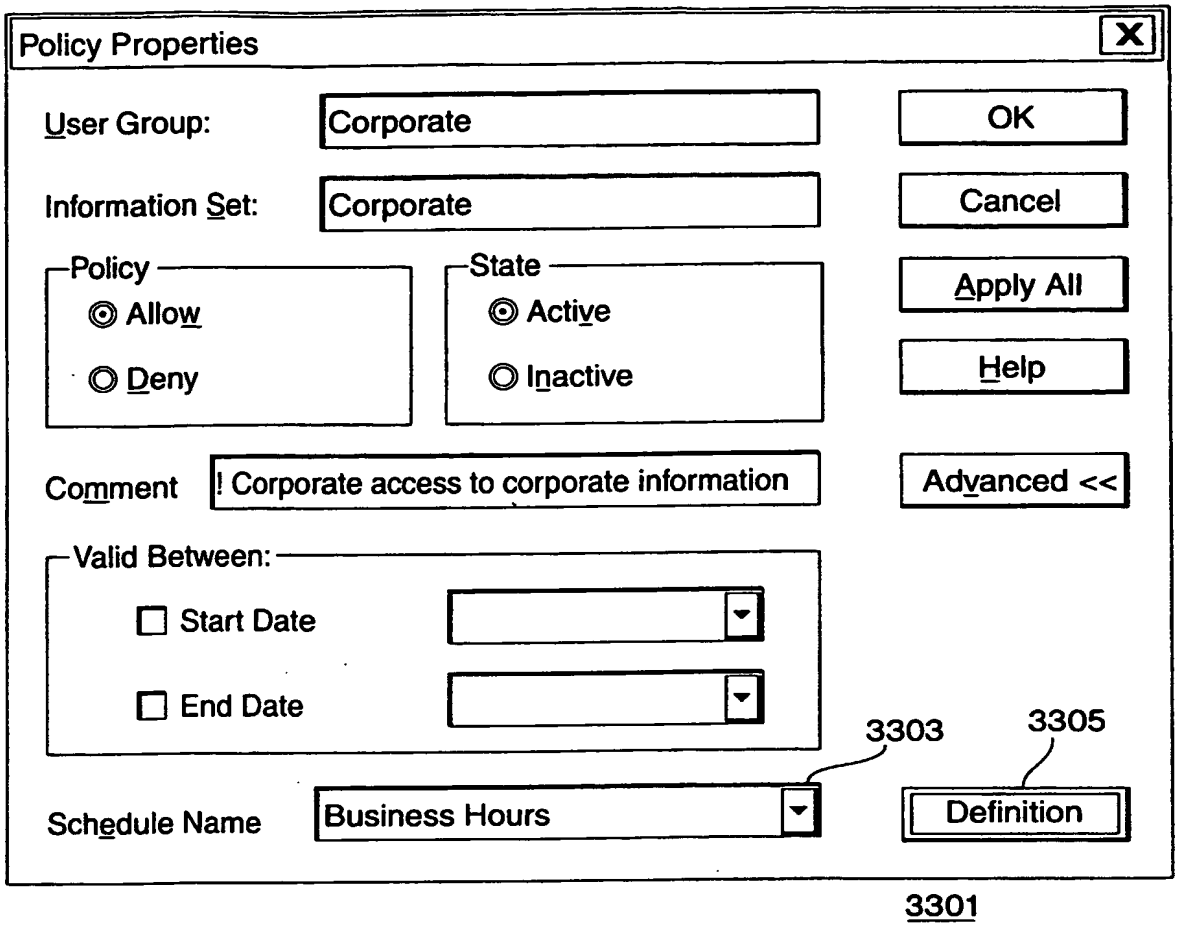

Policy Properties
User Group:
Corporate
Information Set:
Corporate
Policy
Allow
Deny
State
Active
Inactive
Comment
! Corporate access to corporate information
Valid Between:
Start Date
End Date
Schedule Name
Business Hours
OK
Cancel
Apply All
Help
Advanced <<
Definition
3303
3305
3301

Fig. 33

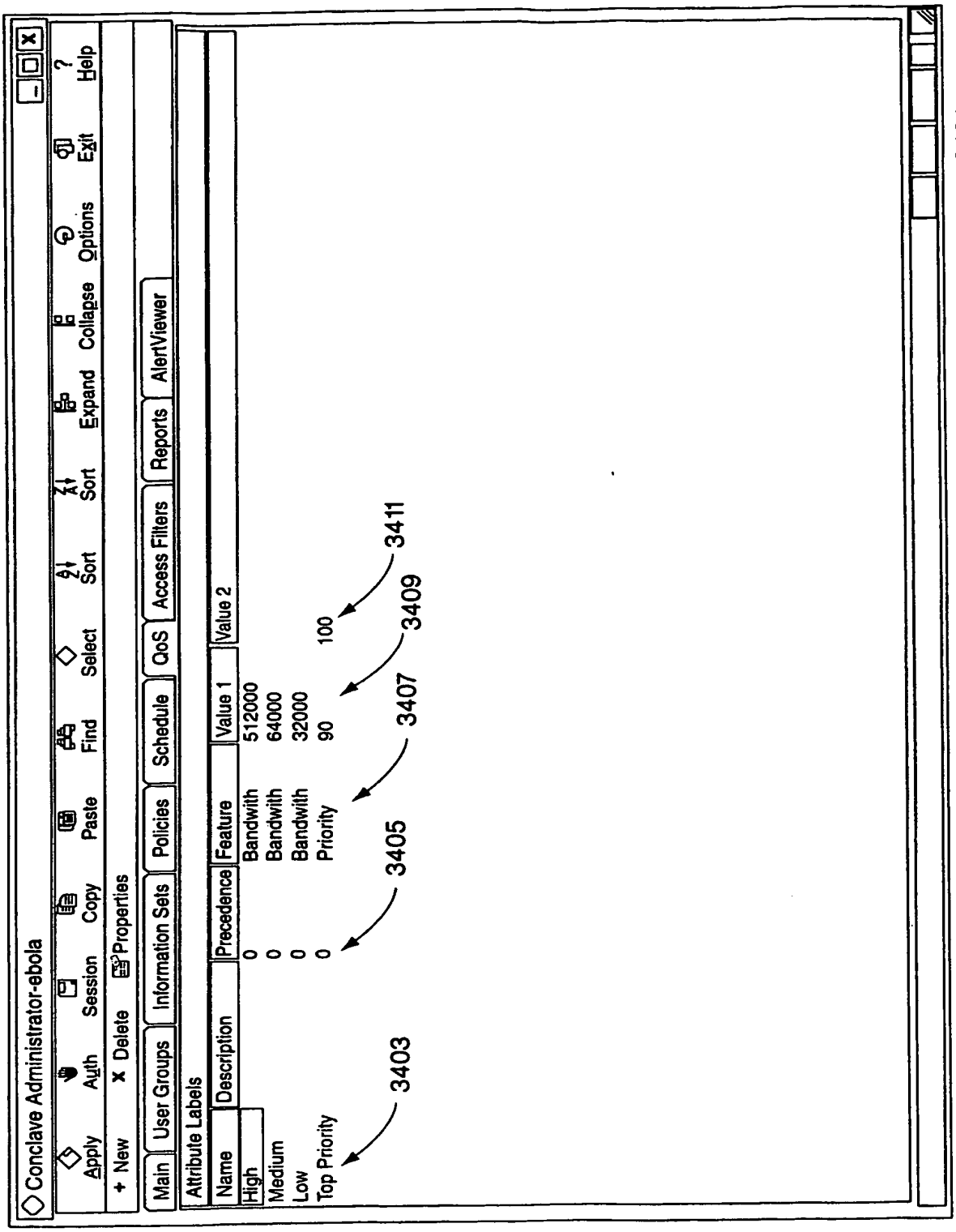


Fig. 34

SUBSTITUTE SHEET

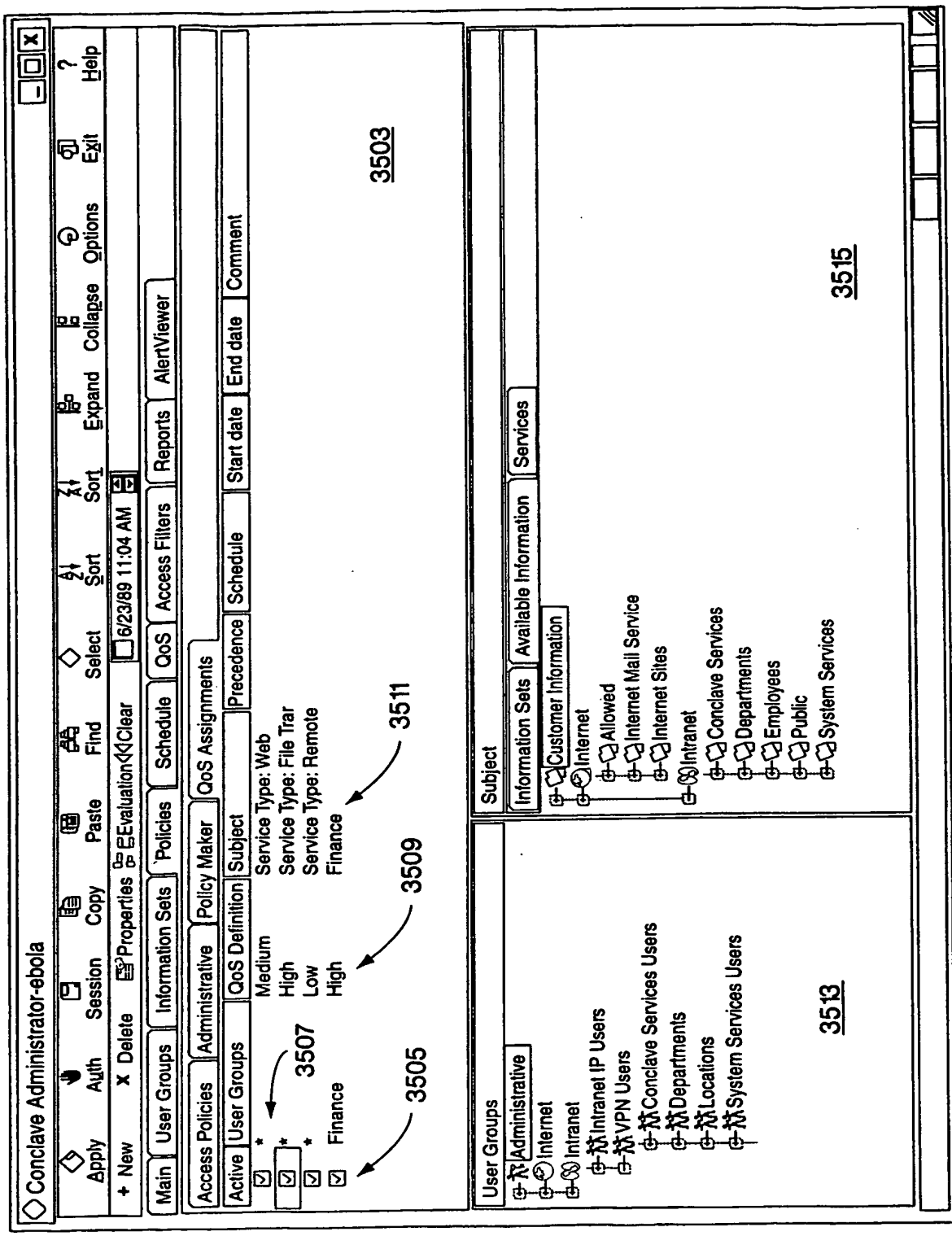

Conclave Administrator-ebola
Apply
Auth
Session
Copy
Paste
Find
Select
Sort
Expand
Collapse
Options
Exit
Help
+ New
Delete
Properties
Evaluation
Clear
6/23/89 11:04 AM
Main
User Groups
Information Sets
Policies
Schedule
QoS
Access Filters
Reports
AlertViewer
Access Policies
Administrative
Policy Maker
QoS Assignments
Active
User Groups
QoS Definition
Subject
Precedence
Schedule
Start date
End date
Comment
Medium
High
Low
High
Service Type: Web
Service Type: File Trar
Service Type: Remote
Finance
3503
3507
3511
3509
3505
User Groups
Administrative
Internet
Intranet
Intranet IP Users
VPN Users
Conclave Services Users
Departments
Locations
System Services Users
3513
Subject
Information Sets
Available Information
Services
Customer Information
Internet
Allowed
Internet Mail Service
Internet Sites
Intranet
Conclave Services
Departments
Employees
Public
System Services
3515
3501

Fig. 35

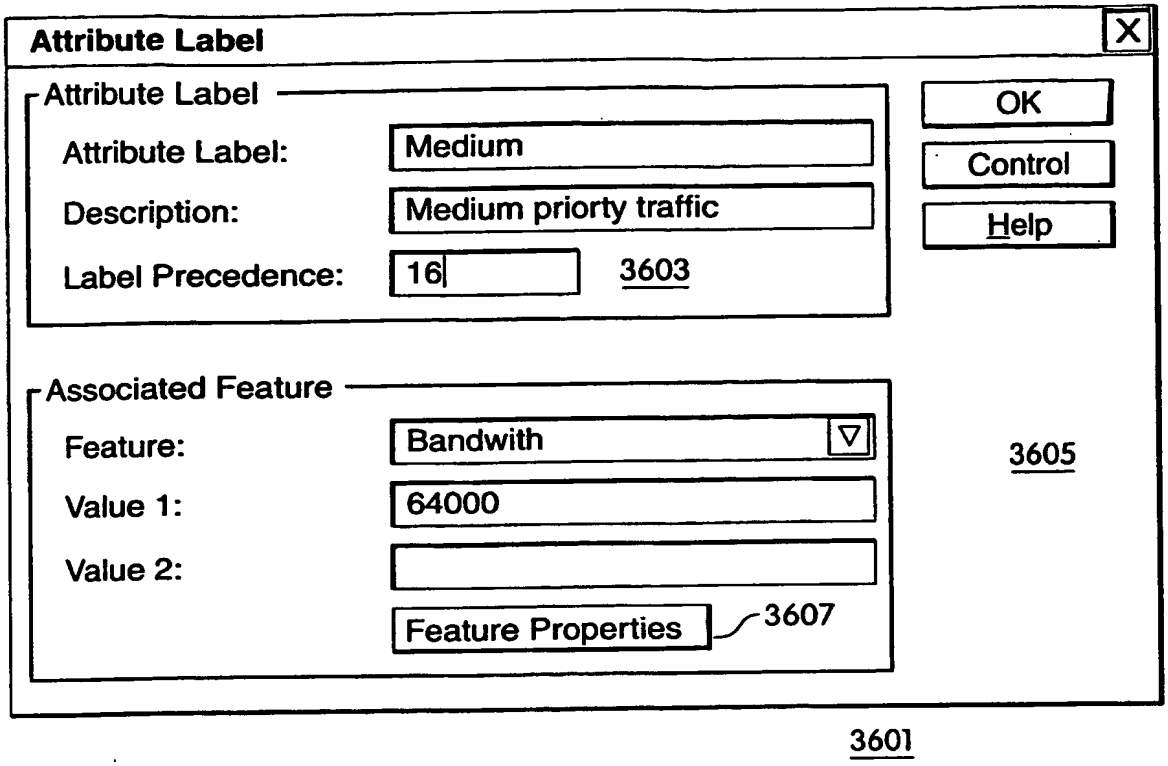

Attribute Label
Attribute Label
Attribute Label:
Medium
Description:
Medium priorty traffic
Label Precedence:
16
3603
OK
Control
Help
Associated Feature
Feature:
Bandwith
Value 1:
64000
Value 2:
Feature Properties
3607
3605
3601

Fig. 36

10/019101

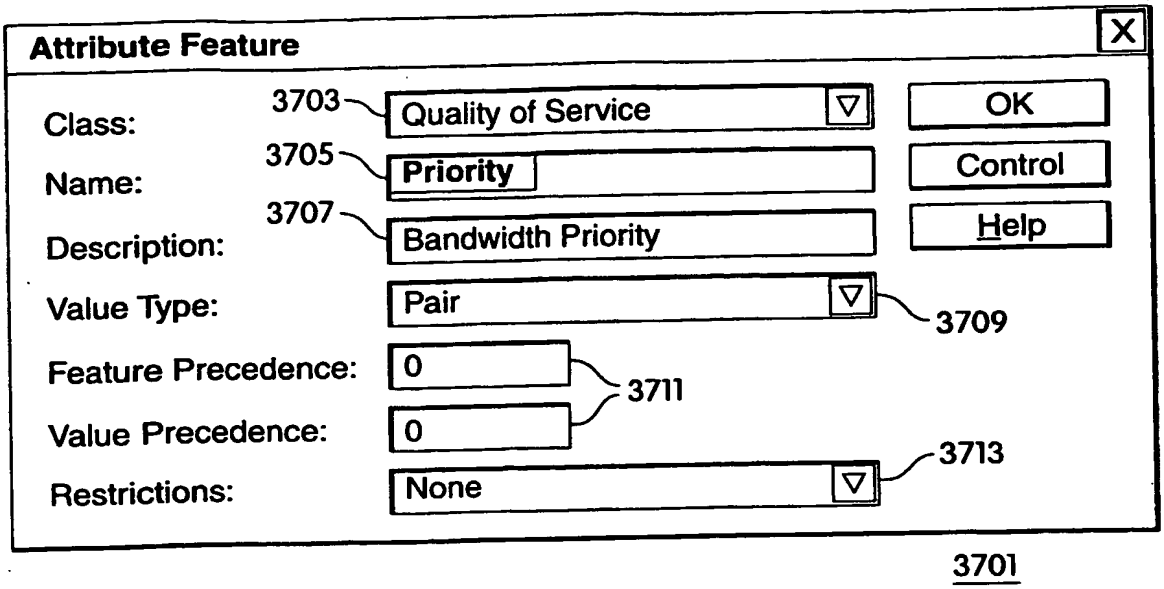
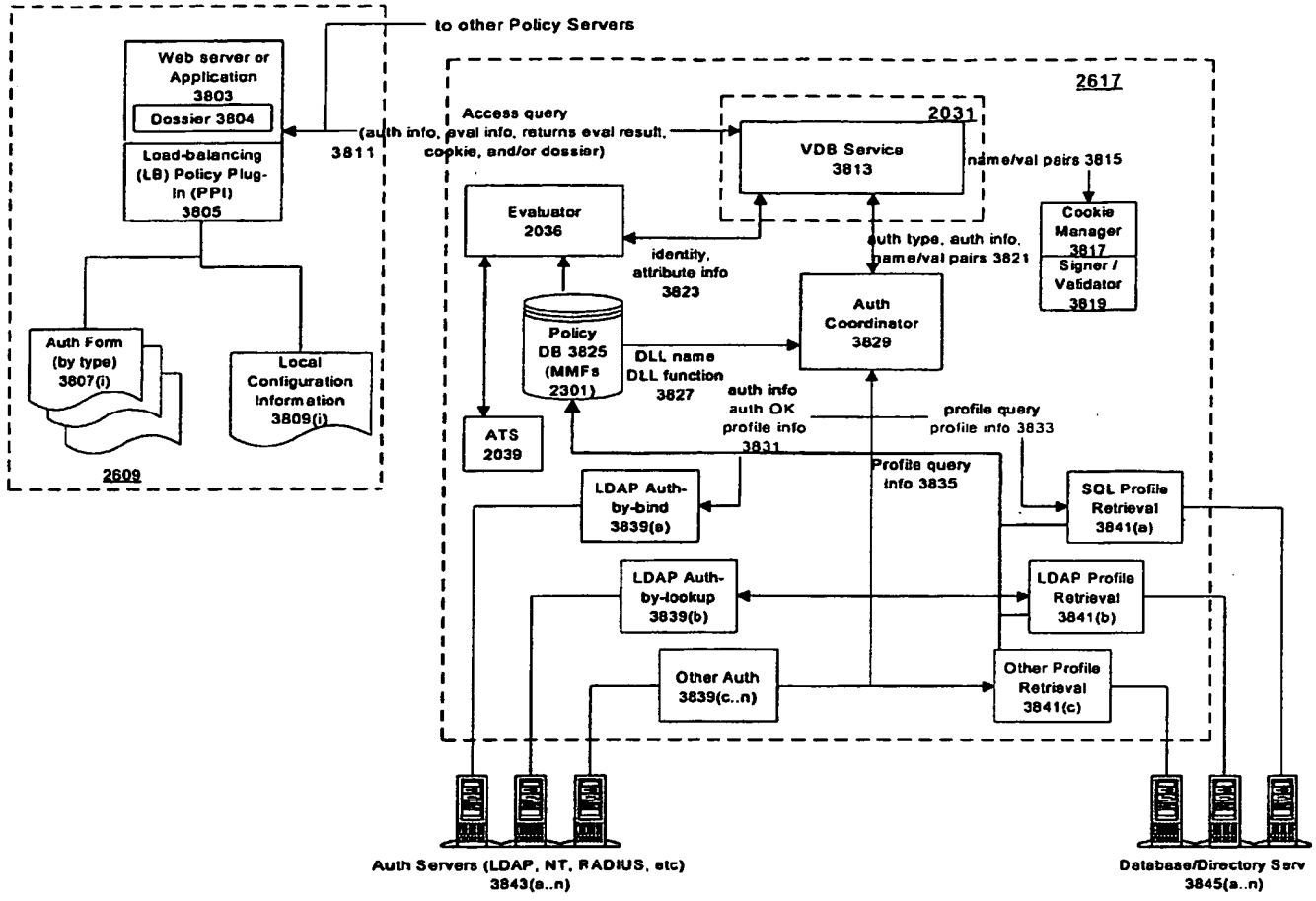


Fig. 37

Replacement Sheet - 11/2001

10/019101



3801

FIG. 38

SUBSTITUTE SHEET (RULE 26)

1U/019101

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD W3 HTML//EN">
<html>

<head>
<meta content="text/html; charset=unicode" http-
equiv="Content-Type">
<!-- #include file="psquery.inc" -->
<title>Policy Query Example</title>
</head>

<body>

<h1>Conclave Policy Enabled Page</h1>
<%
   if ConclavePolicyAllowed() = "Yes" then
      'Put the allowed action here
      Response.Write "<p>You've been allowed to this
page.</p>"
   else
      'Put denied action here
      Response.Write "<p>You've been <b>denied</b> to this
page.</p>"
   end if
%>

<p> </p>
</body>
</html>
```

3903

3905

3907

3901

FIG. 39

```
<%
'%%%
```

10/019101

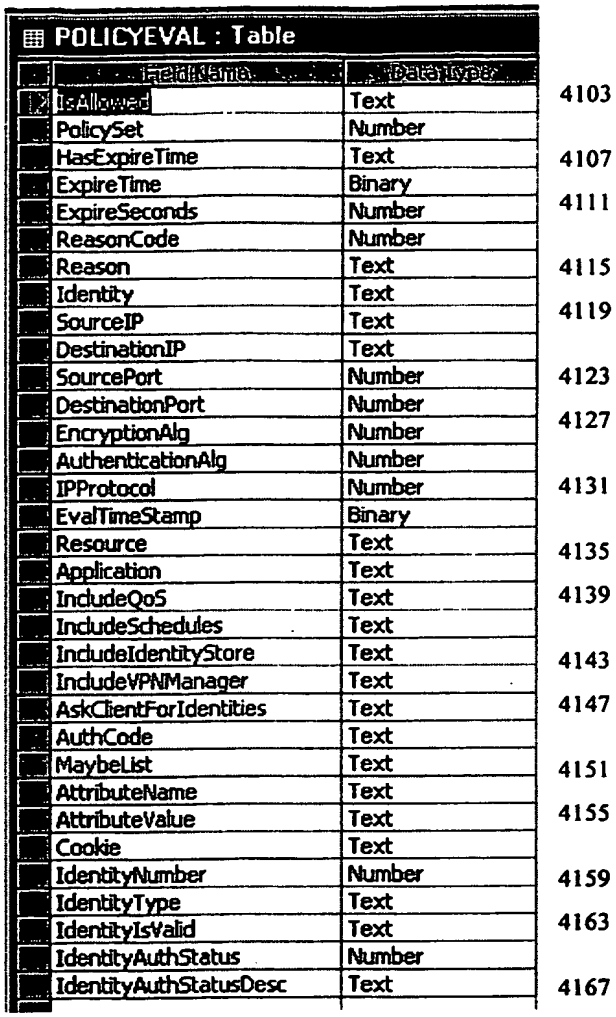


FIG. 41

```
SELECT IsAllowed, PolicySet, HasExpireTime, ExpireTime, Reason from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80                                    4203
AND EncryptionAlg = 64
AND AuthenticationAlg = 2
AND IPProtocol = 6
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'
```

IsAllowed	PolicySet	HasExpireTime	ExpireTime	Reason
Y	56	N	1969-12-31 16:00:00	None

4205

4201

```
SELECT IsAllowed, Reason from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80
AND EncryptionAlg = 64
AND AuthenticationAlg = 2
AND IPProtocol = 6                                          4209
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'
```

IsAllowed	Reason
Y	None

4211

4207

```
SELECT * from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND SourcePort = 0
AND DestinationIP = '172.31.1.32'
AND DestinationPort = 80
AND EncryptionAlg = 64                                      4213
AND AuthenticationAlg = 2
AND IPProtocol = 6
AND EvalTimeStamp = '07-JUL-1999 13:39:34'
AND Resource = 'Conclave/ConclaveEval.html'
```

```
SELECT IsAllowed, PolicySet, HasExpireTime, ExpireTime, Reason from PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'                           4217
AND Resource = 'Conclave/ConclaveEval.html'
```

IsAllowed	PolicySet	HasExpireTime	ExpireTime	Reason
Y	56	N	1969-12-31 16:00:00	None

4219

4215

FIG. 42

```
SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'                    4303
AND Resource = 'Conclave/ConclaveEval.html'
```

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4305

4301

```
SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'                    4309
AND Resource = 'Conclave/ConclaveEval.html'
AND IdentType = 'CertificateDN'
AND IdentValue = '/O=XYZ/OU=Engineering/CN=JoeUser'
```

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4311

4307

```
SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'                    4315
AND Resource = 'Conclave/ConclaveEval.html'
AND IncludeIdentityStore = 'Y'
```

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4317

4313

```
SELECT IsAllowed, Reason, IdentType, IdentGroup, IdentValue from
PolicyEval
WHERE SourceIP = '172.31.1.31'
AND DestinationIP = '172.31.1.32'
AND Resource = 'Conclave/ConclaveEval.html'                    4321
AND IncludeIdentityStore = 'Y'
AND IdentType NOT IN ( 'WindowsID','Radius','IP' )
```

IsAllowed	Reason	IdentType	IdentGroup	IdentValue
Y	Allowed by Certificate	CERTIFICATEDN	1	/O=XYZ
Y	Allowed by Certificate	CERTIFICATEDN	1	/OU=Engineering
Y	Allowed by Certificate	CERTIFICATEDN	1	/CN=JoeUser

4322

4319

FIG. 43

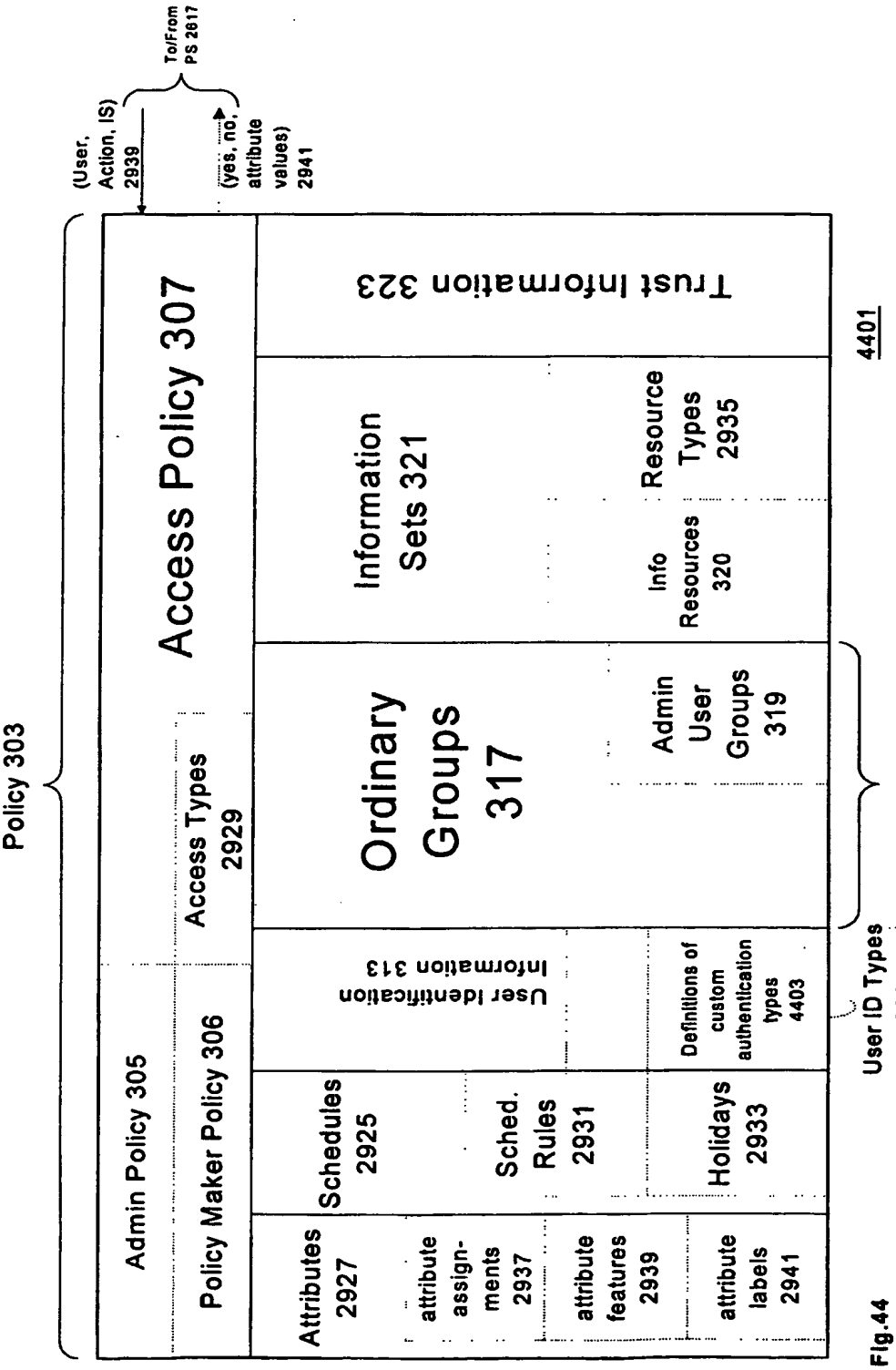
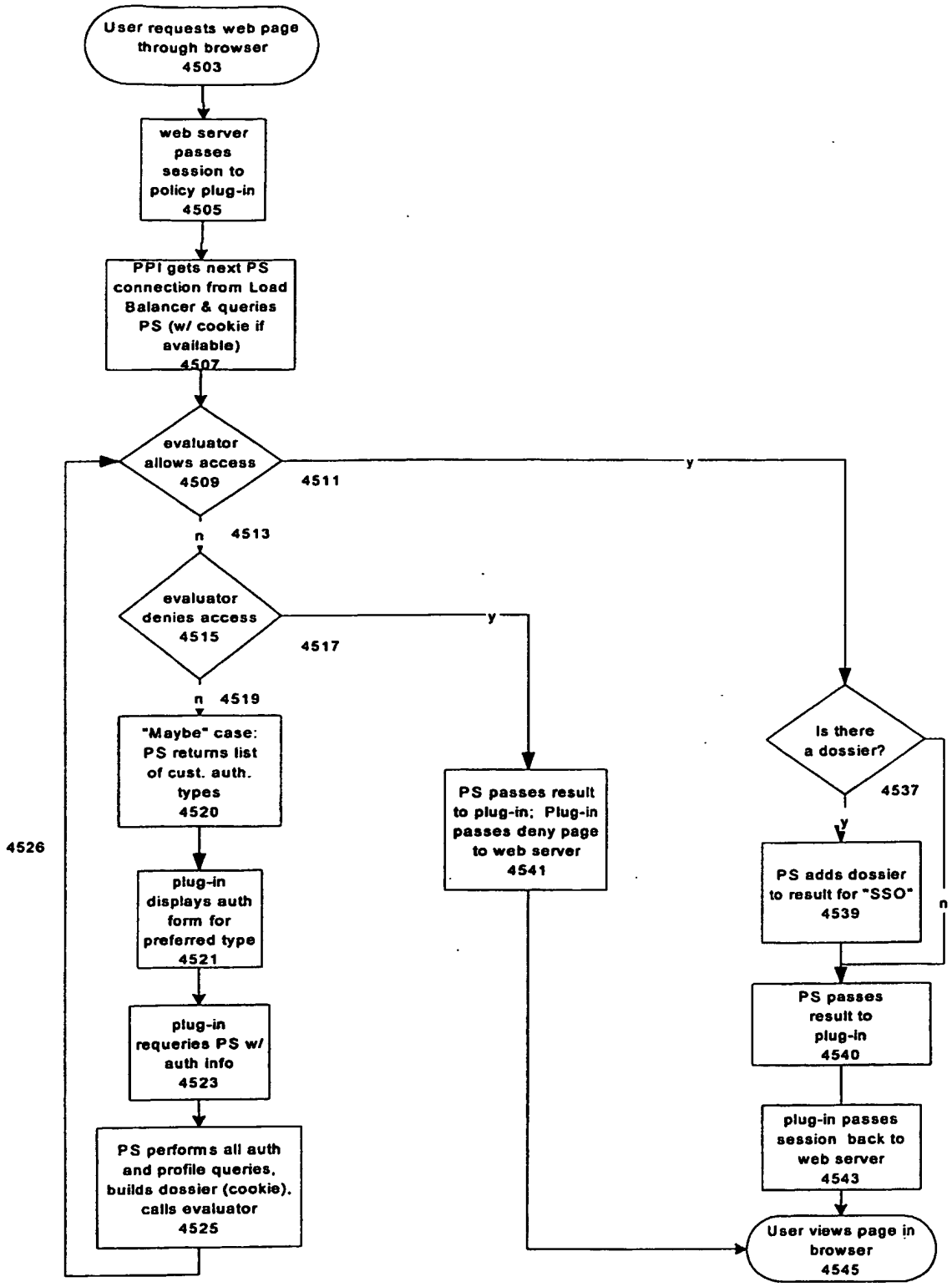

Policy 303
Admin Policy 305
Policy Maker Policy 306
Access Policy 307
Access Types 2929
Ordinary Groups 317
Admin User Groups 319
Information Sets 321
Info Resources 320
Resource Types 2935
Trust Information 323
User Identification Information 313
Definitions of custom authentication types 4403
Attributes 2927
attribute assign-ments 2937
attribute features 2939
attribute labels 2941
Schedules 2925
Sched. Rules 2931
Holidays 2933
(User, Action, IS) 2939
(yes, no, attribute values) 2941
To/From PS 2817
User ID Types 2937
User Groups 315
4401

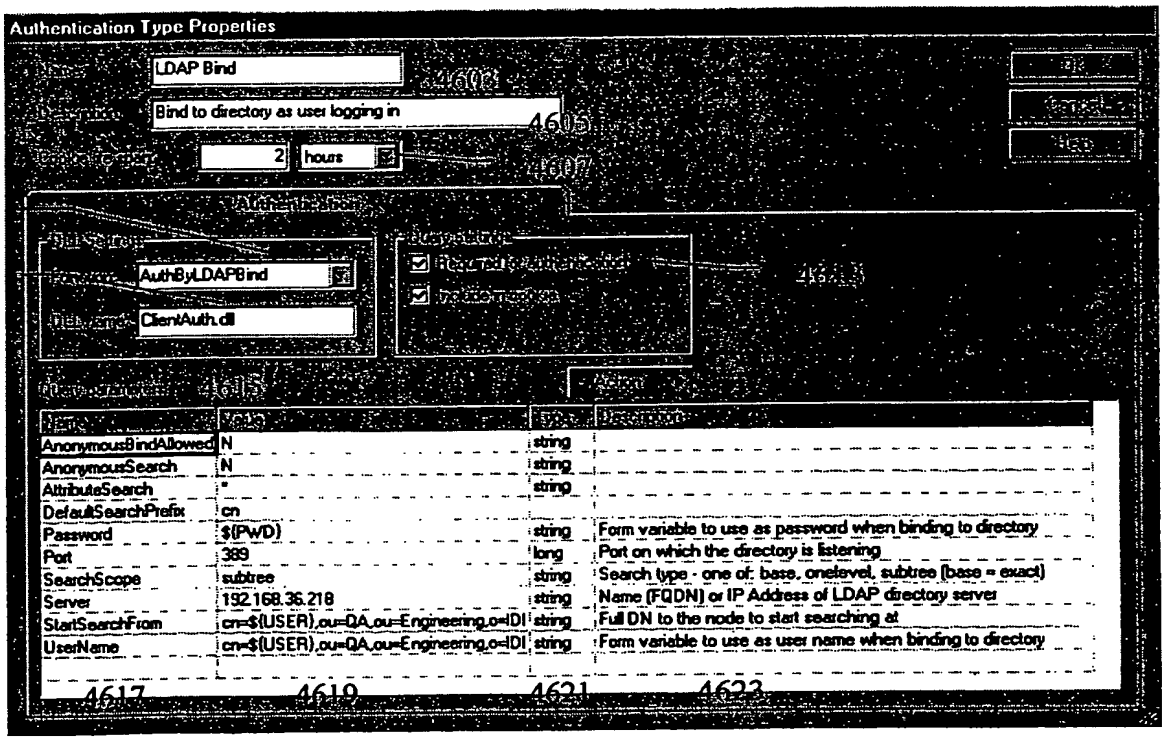
Fig.44


User requests web page through browser 4503
web server passes session to policy plug-in 4505
PPI gets next PS connection from Load Balancer & queries PS (w/ cookie if available) 4507
evaluator allows access 4509
4511
y
n
4513
evaluator denies access 4515
4517
y
n
4519
"Maybe" case: PS returns list of cust. auth. types 4520
plug-in displays auth form for preferred type 4521
plug-in requeries PS w/ auth info 4523
PS performs all auth and profile queries, builds dossier (cookie), calls evaluator 4525
4526
PS passes result to plug-in; Plug-in passes deny page to web server 4541
Is there a dossier?
4537
y
n
PS adds dossier to result for "SSO" 4539
PS passes result to plug-in 4540
plug-in passes session back to web server 4543
User views page in browser 4545

4501

FIG. 45

10/019101



4601

FIG. 46

10/019101

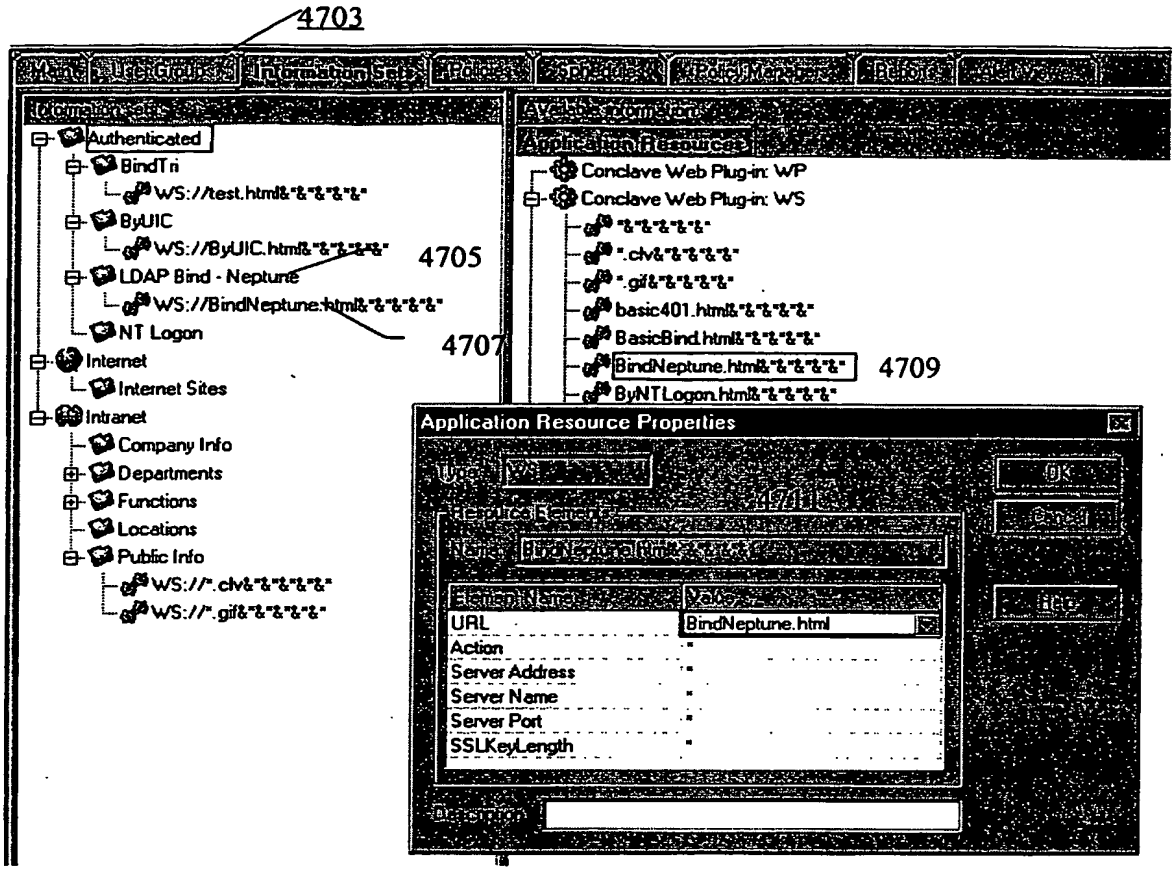


FIG. 47

SUBSTITUTE SHEET (RULE 26)

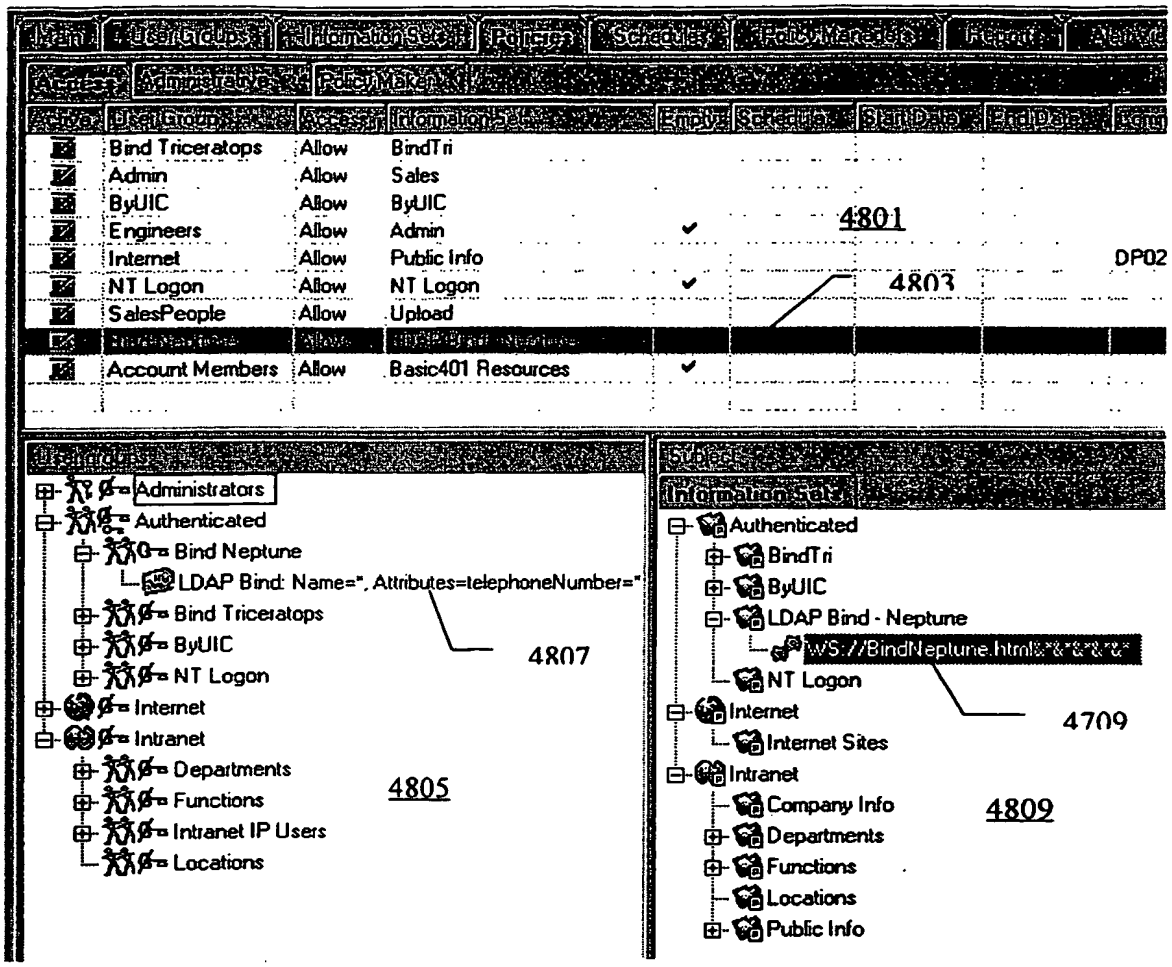

Bind Triceratops Allow BindTri
Admin Allow Sales
ByUIC Allow ByUIC
Engineers Allow Admin
Internet Allow Public Info
NT Logon Allow NT Logon
SalesPeople Allow Upload
Account Members Allow Basic401 Resources
4801
4803
DP02
Administrators
Authenticated
Bind Neptune
LDAP Bind: Name=", Attributes=telephoneNumber="
Bind Triceratops
ByUIC
NT Logon
Internet
Intranet
Departments
Functions
Intranet IP Users
Locations
4807
4805
Information Set
Authenticated
BindTri
ByUIC
LDAP Bind - Neptune
NT Logon
Internet
Internet Sites
Intranet
Company Info
Departments
Functions
Locations
Public Info
4709
4809

FIG. 48

SmartCard Types : Table

	SmartCardTyp	Type	Manufacturer	Version	Number
▶	947715536	LDAPBind	Bind to an LDAP Server to authenticate a users identity	1	3
*	(AutoNumber)				0

4903 4905 4907

4901

Proxy Definitions : Table

	ProxyTypID	Name	Description	Type	RecordSize	Details	PreDefined	ParametersNumber
▶	344148459	LDAPBind	Web service proxy	1	1		0	50
*	AutoNumber)				0		0	0

4911 4913 4915 4917

4909

FIG. 49

Proxy Parameter Definitions : Table

ProxyParamID	ProxyPathID	Name	Description	Value
-1287839664	344148459	Cookie TTL	Cookie time to live in [seconds]	2580
-255422959	344148459	Queries	Defined queries	Step1,Step2
581256871	344148459	Step1/DLL Function	Function name in query DLL	LDAPBindAuth
-1513472258	344148459	Step1/DLL Name	Query's DLL name	ClientAuth.DLL
704661805	344148459	Step1/Include In Cookie	Include query results in cookie	1
-838120726	344148459	Step1/Maximum Execution Time	Maximum query execution time in [seconds]	0
922587944	344148459	Step1/Port		389
1170892639	344148459	Step1/ProfileAttribute		Room*
237910181	344148459	Step1/ProfileAttribute		WorkPhone*
1513326004	344148459	Step1/ProfileAttribute		EM*
994538844	344148459	Step1/Required	Query is required for authentication	1
97150755	344148459	Step1/Server		betelgeuse
2127089161	344148459	Step1/UserDN		${UserID}
-945271402	344148459	Step1/UserPwd		${UserPwd}
1498465115	344148459	Step2/DLL Function	Function name in query DLL	GetNTUserGroups
-1253821694	344148459	Step2/DLL Name	Query's DLL name	ClientAuth
423126273	344148459	Step2/Include In Cookie	Include query results in cookie	1
350791470	344148459	Step2/Maximum Execution Time	Maximum query execution time in [seconds]	0
412661527	344148459	Step2/NTDomain		INTERDYN
-1837754112	344148459	Step2/Required	Query is required for authentication	0
437704972	344148459	Step2/UserID		${UserID}
604303133	344148459	Step2/UserPwd		${UserPwd}

5002 5003 5005 5007 5009 5011 5013 5015 5016 5017 5019 5021 5023

5001

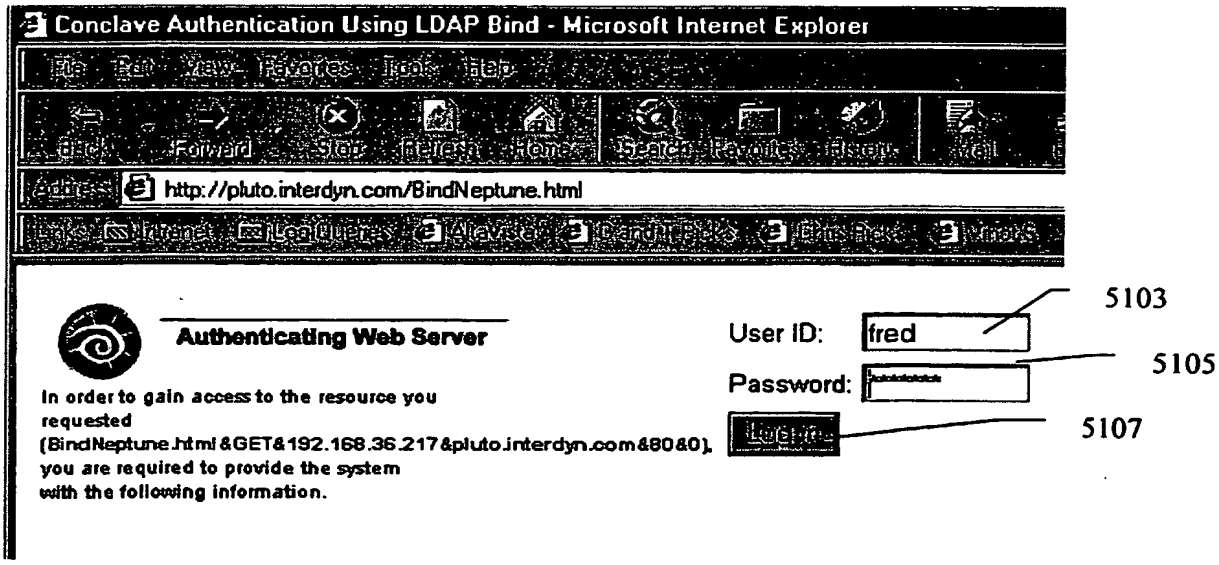
Smartcard Definitions : Table

SmartCardDefID	Name	TypeID	Code	Description
-1175318968	TonyM	947715538		RoomNumber=2236*
(AutoNumber)		0		

5027 5029 5031 5033

5025

FIG. 50


Conclave Authentication Using LDAP Bind - Microsoft Internet Explorer
http://pluto.interdyn.com/BindNeptune.html
Authenticating Web Server
In order to gain access to the resource you requested (BindNeptune.html&GET&192.168.36.217&pluto.interdyn.com&80&0), you are required to provide the system with the following information.
User ID:
fred
Password:
5103
5105
5107

5101

FIG. 51

```
select Cookie,IdentityIsValid, IsAllowed, reasoncode,
     maybelist, cookiemodified
from policyeval
where sourceip='192.168.36.215' and
     application='WS' and
     resource='BindNeptune.html&GET&192.168.36.217&
          pluto.interdyn.com&80&0'
     and includeeval='Y' and
     includeidentitystore='Y' and
     askclientforidentities='N' and
     identity= 'AUTHPOSTIDENTITY IDENTTYPE="LDAP Bind"&
          ORIGINALURL="BindNeptune.html&GET&
          192.168.36.217&pluto.interdyn.com&80&0"&
          AUTHTYPE="LDAP Bind"&USER="fred"&PWD="agent99"&
          SUBMIT1="Log in"'
```

5203 5204 5205 5207 5209 5211 5201

FIG. 52

5303

```
Cookie=CONCLAVE=COOKIEIDENTITY=COOKIEIDENTITY%26AUTHTYPE%
    3D%22LDAP%20Bind%22%26IDENTTYPE%3D%22LDAP%20Bind%
    22%26ORIGINALURL%3D%22BindNeptune.html%26GET%
    26192.168.36.217%26pluto.interdyn.com%2680%260%
    22%26SUBMIT1%3D%22Log%20in%22%26USER%3D%22fred%
    22%26UserName%3D%22cn%3Dfred%2Cou%3DQA%2Cou%
    3DEngineering%2Co%3DIDI%22&EXPIRES=Thu%2C%
    2008-Jun-2000%2000:28:41%20GMT&cn=fred&
    facsimileTelephoneNumber=805-666-5563&
    initials=ddf&mail=fred@interdyn.com&objectClass=top&
    objectClass=person&objectClass=organizationalPerson&
    objectClass=inetOrgPerson&roomNumber=2217&sn=user&
    telephoneNumber=805-652-2544&uid=fred&
    NONCE=f+7KBJmHR6/XWCTmREhmnQ&   5305
    SIG=qd0ZLcPBjMiPbGlR7C7urAXad2Q; 5307
    EXPIRES=Thu, 08-Jun-2000 00:28:41 GMT;
    MAX-AGE=960424121;
IdentityIsValid = Y    5309
IsAllowed = Y  5311
ReasonCode = 116
MaybeList =    5313
CookieModified = Y
```

5301

FIG. 53

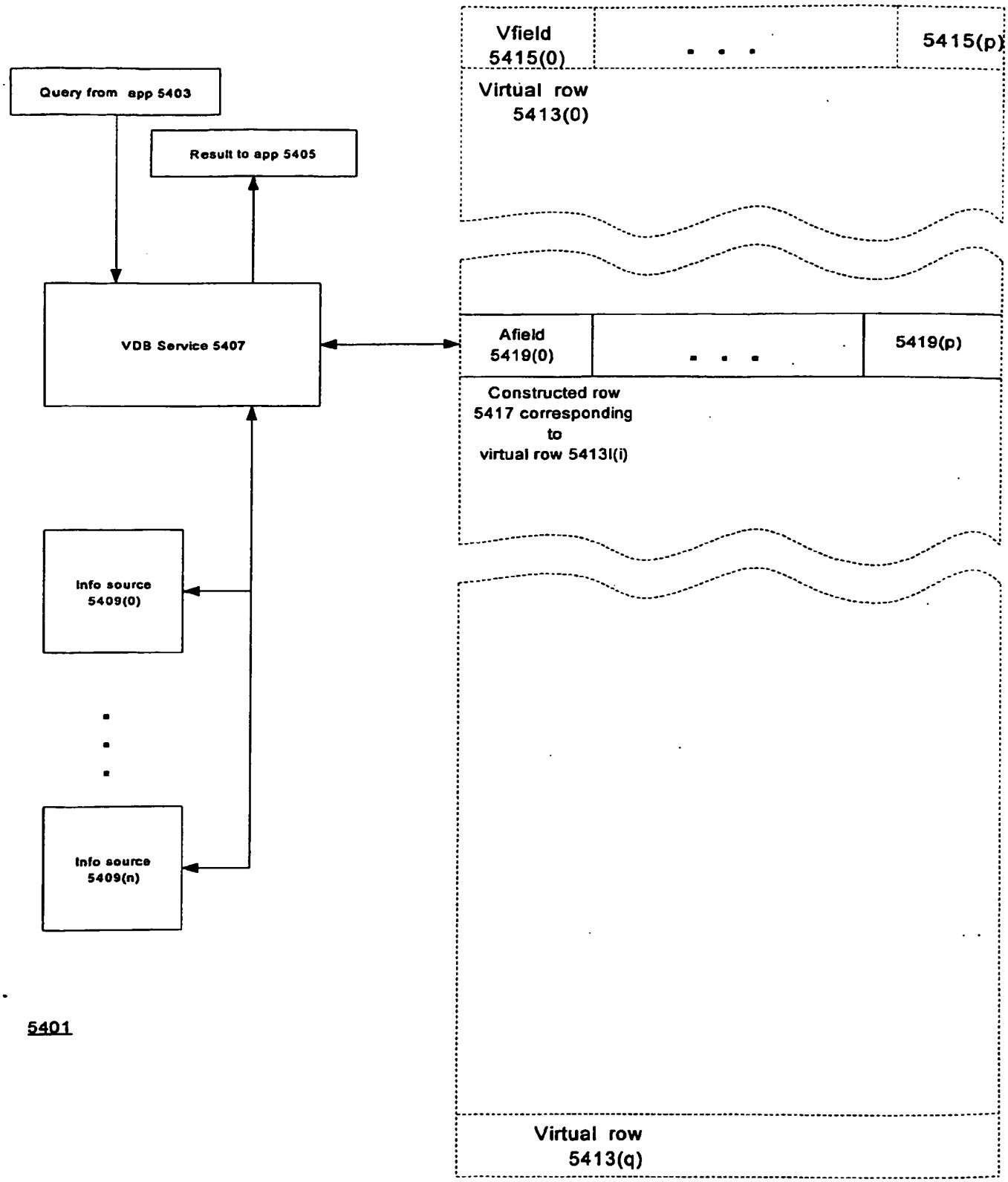

Query from app 5403
Result to app 5405
VDB Service 5407
Info source 5409(0)
Info source 5409(n)
5401
Vfield 5415(0)
5415(p)
Virtual row 5413(0)
Afield 5419(0)
5419(p)
Constructed row 5417 corresponding to virtual row 5413I(i)
Virtual row 5413(q)
Virtual relational database table 5411

FIG. 54